ATEUS ® - Remote Control Unit

RCU

User's Guide

Version: 5.00

CONTENTS

1 INTRODUCTION 3

1.1 MANAGEMENT 3

1.1.1 Control 3

1.1.2 Monitoring 4

1.2 ACCOUNTING 4

1.2.1 Call Data Record (CDR) 4

1.2.2 Traces 4

1.2.3 Logs 4

1.2.4 Call statistics 5

1.3 EXTERNAL ROUTING 5

2 THE RCU SYSTEM 7

2.1.1 The basic system 7

2.1.2 The communication protocols 7

2.1.3 The Management Services Engines 7

2.1.4 The Management Databases 8

3 INSTALLATION 9

3.1 PRE-INSTALLATION 9

3.1.1 Topology 9

3.1.2 Assigning IP addresses 9

3.2 OS INSTALLATION 10

3.2.1 Installation procedure 10

4 CONFIGURATION 11

4.1 BASIC CONFIGURATION 11

4.1.1 E-mail alarms 12

4.1.2 SMS alarms 12

4.1.3 Call Data Records (billing) 13

4.1.4 The ASR statistics 13

4.1.5 Utilization of PRI ports 13

4.1.6 The PRI GSM gateways 14

4.1.7 Network Address Translation 15

4.1.8 SNMP Configuration 15

4.1.9 Binding PRI GSM Gateways to databases 15

4.1.10 External routing 16

4.1.11 Alarm filtering 16

4.2 WEB ACCESS CONFIGURATION 17

4.3 TESTING 18

4.4 CONFIGURATION EXAMPLE 18

4.4.1 IP map Table 18

4.4.2 Configuration 19

4.4.3 Web pass 21

4.4.4 Starting 22

4.4.5 Testing 22

5 RCU USAGE 24

5.1 WEB ACCESS 24
5.1.1 Welcome Message 24
5.1.2 Authentication 25
5.1.3 Web Overview 25
5.1.4 Web configuration of the gateway 28
5.1.5 Incomming Call Simulation 28
5.2 SNMP MANAGEMENT 29
5.2.1 SNMP Queries 29
5.2.2 SNMP Traps 29
5.3 ACCOUNTING 30
6 TROUBLESHOOTING 32
6.1 STARGATE SERVICE 32
6.2 GATEWAY CONFIGURATION (SGCONF) 32
6.3 CHECKING THE DATABASES 33
6.3.1 Gateway Databases 33
6.3.2 Gateway Terminal (sgterm) 33
6.3.3 Accessing table main 33
6.4 STARGATE (BLUESTAR) PROGRAM USING RCU AS A TUNNEL 35
6.5 TRACING OF THE TRAFFIC ON GATEWAYS 37
7 FAQ 38
APPENDIX 1: THE TRAP TABLE 39

1 Introduction

Unlike the most of telecommunications devices that come with integrated remote management modules, PRI GSM gateways produced by 2N Telekomunikace a.s, the *ATEUS* ® STARGATE (Stargate) and *ATEUS* ® BLUESTAR (Bluestar) come with a Remote Control Unit (RCU), a standalone device offering a wider range of management and accounting capabilities. The RCU was originally developed to provide management of Stargate. The new version 2.0 supports both types of PRI GSM gateways. **This User's Guide references to RCU ver. 4.00** and **higher.** Though the most of commands or database names remind on Stargate, as the RCU original goal, the RCU could be used for both gateways.

IMPORTANT!!!

RCU ver. 4.00 and higher requests Stargate (Bluestar) firmware version 2.16.43 or higher.

1.1 Management

One RCU can manage up to eight PRI GSM gateways.

1.1.1 Control

The RCU supports a number of methods for querying and or changing the PRI GSM gateways' parameters:

- *Web interface*: From the common web browser, customers can alter configuration parameters in their PRI GSM gateways on the fly (**Web configuration**).
- *Simple Network Management Protocol (SNMP)*: Designed to proxy PRI GSM gateways to most commonly used network management software, The RCU allows clients to send legacy SNMP queries.
- *Secure AT shell*: The PRI GSM gateway supports a set of AT commands. To send these commands to the PRI GSM gateways remotely, one has to use telnet, an insecure remote login protocol. The RCU nails this problem such that, over the insecure Internet, telnet traffic is tunneled through Secure Shell (SSH) and only allowed in the LAN where the climate is relatively friendly. This allows clients to send configuration or query commands to the managed PRI GSM gateways without having to worry that an evil cracker could be tapping the communication (see Fig.1).

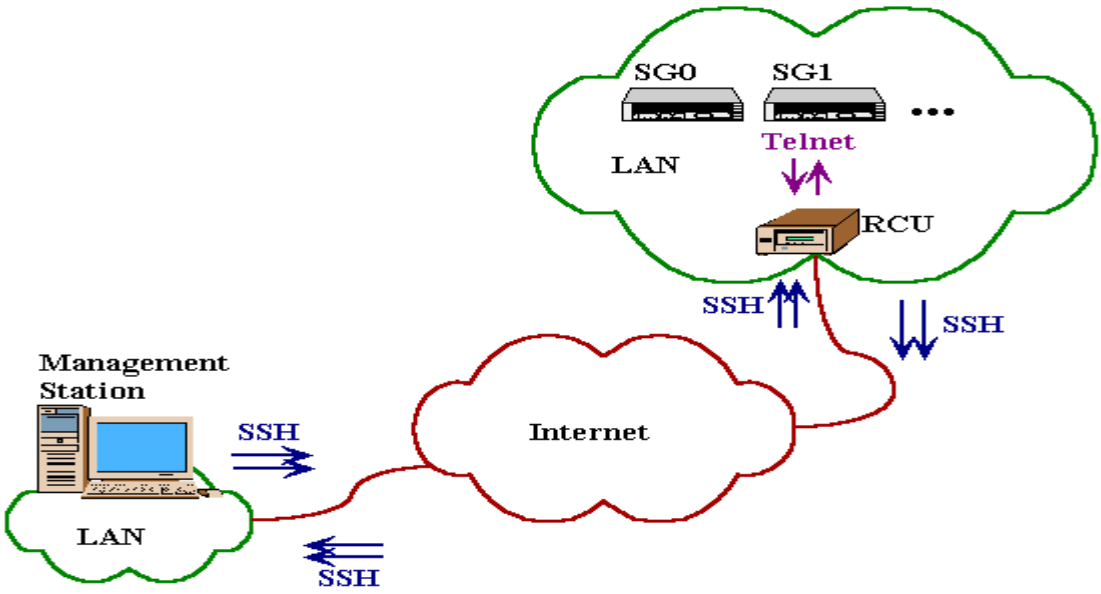

Fig.1: AT command tunneling over SSH

1.1.2 Monitoring

The RCU comes with a number of PRI GSM gateway monitoring methods:

- *Web interface*: over the WWW, clients can monitor their PRI GSM gateways while comfortably sitting in their offices. Occurrences of undesired (erroneous) conditions are promptly indicated by changes of color in the offending modules.
- *Simple Network Management System (SNMP)*: The RCU continuously monitors the attached PRI GSM gateways and sends an SNMP trap every time a non standard status is observed
- *E-mail*: The RCU can be configured to send an email alarm in event that a PRI GSM gateway or one of its components fails
- *SMS*: The RCU is also capable of sending an SMS alarm when so configured, to announce faults in the managed devices.

1.2 Accounting

The RCU is equipped with a number of databases and processes that collect and archive call accounting data

1.2.1 Call Data Record (CDR)

The RCU periodically collects CDRs from the PRI GSM gateways and stores them in its local disk. This removes the risk that these records would be overwritten when the PRI GSM gateway buffers are filled. These CDRs are accessible through the web.

1.2.2 Traces

The RCU automatically reroutes all the PRI GSM gateway call traces to its local disk. These traces come in handy when troubleshooting a non standard status. They can also be accessed over the web.

1.2.3 Logs

The RCU also stores status logs on all the PRI GSM gateway management applications. These are again useful when diagnosing management problems.

1.2.4 Call statistics

The RCU stores call summaries. These can be either overall or based on differed modules and SIM cards. The call statistics are readily available over the web

1.3 External Routing

The PRI GSM gateway is equipped with an additional capability to route calls based on an external routing database – the so-called External Routing. This design opens the doors to the PRI GSM gateway, to take advantage of the greater capacities of external routing databases as opposed to its limited internal routing buffers. The RCU, as we shall see, has a special database for this purpose. To use this special function, a routing database (LCR) has to be installed into the RCU. This database contains a table *rtlist*. Each record in database contains destination phone number and a number of the outgoing GSM group, the call should be routed through. If the group number is 0, call will be rejected i.e. that number is on "blacklist". If the group number is 9, call will be routed to the second PRI port of the gateway (PRI2).

External routing works in such a way that, when a call comes into the PRI GSM gateway either from the PRI interface (SETUP) or from the GSM network (RING), the PRI GSM gateway opens a telnet connection to the RCU and requests for instructions on how to route the call. This request is of the form ***ring: ch,cref,dial,clip** where:

- Ch – module number (0-31) or PRI channel 97-111 and 113-127 (timeslot +96)
- Cref – internal call reference number (1-255)
- Dial – called (destination) number
- Clip – callers (source) number

After receiving this message, the first thing the RCU does is that it compares dialed number against the numbers in the table. If there is a match and group number is 0,then the call is rejected with a cause (AT^CR=ch, cref,cause). If on the other hand, group number is 1-9,the RCU returns immediately a return value that contains the group number through which the call will be routed in the PRI GSM gateway (AT^RG=ch,cref,groups). In the case that "dial" is not found in the routing table, the PRI GSM gateway timesout and uses its internal LCR to route the call (Fig.2).

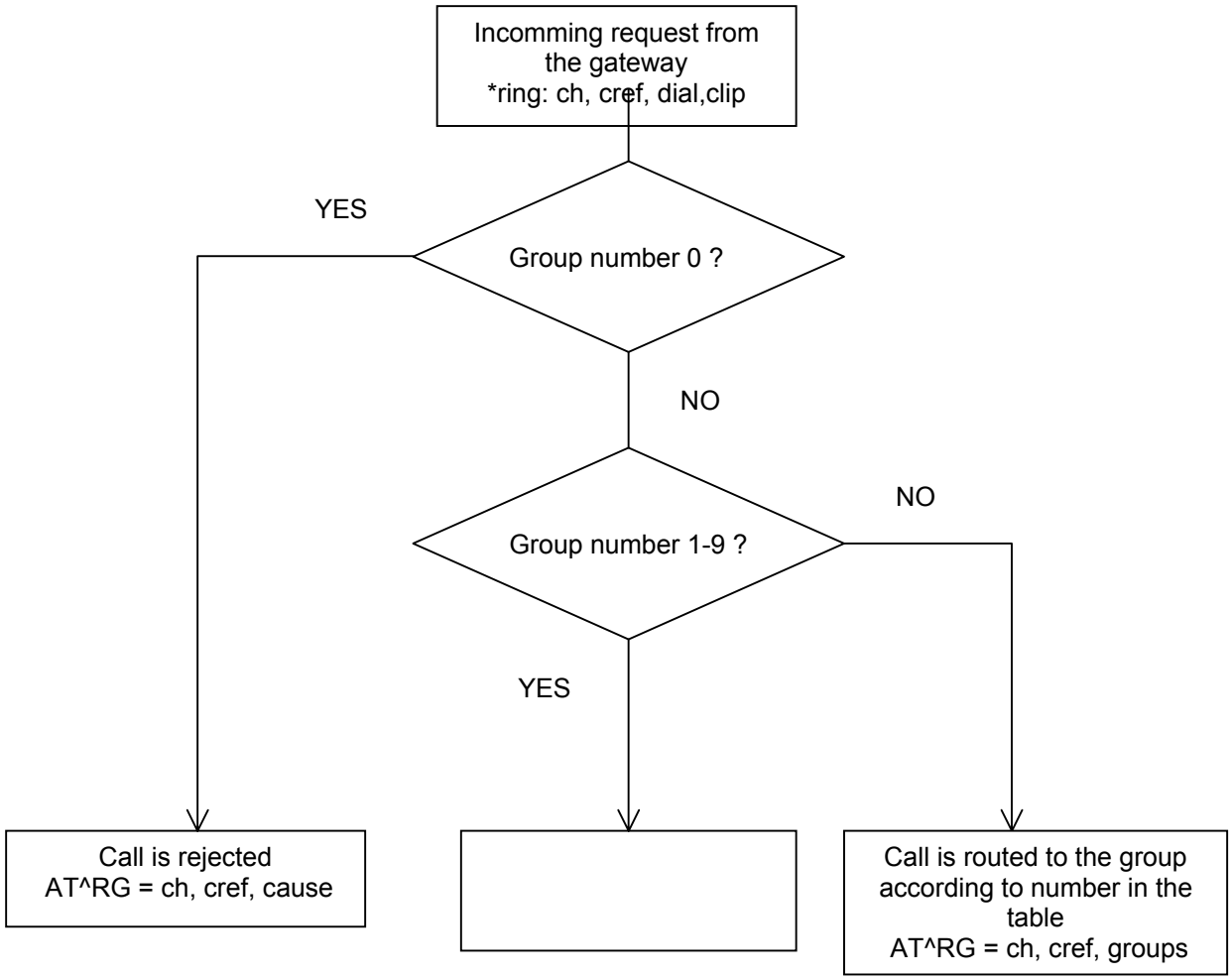

Fig. 2: External routing

2 The RCU System

2.1.1 The basic system

The RCU is made up of a powerful industrial PC running the Linux OS. Linux was specifically chosen to make the system relatively secure.
On top of the Linux OS are a web server (Apache), a database engine (Postgre) and a set of PRI GSM gateway Management and Accounting applications.

2.1.2 The communication protocols

The RCU is equipped with two Ethernet cards usually Eth0 and Eth1. Eth1 connects to the managed PRI GSM gateways' subnet. The RCU uses this interface to communicate with the PRI GSM gateways by telnet or to send SMS in the event of a fault. This arrangement logically isolates the PRI GSM gateways' subnet from the rest of the network and hence using telnet does not open security holes. Eth0 is intended to communicate to the rest of world without making it known that there are PRI GSM gateways hidden on the other side of the wall! The protocols propagated through the firewall include:

- HTTP for web management
- SNMP to provide legacy network management functionality
- SSH for secure remote login
- SMTP sends an email if something happens (see Fig.3).

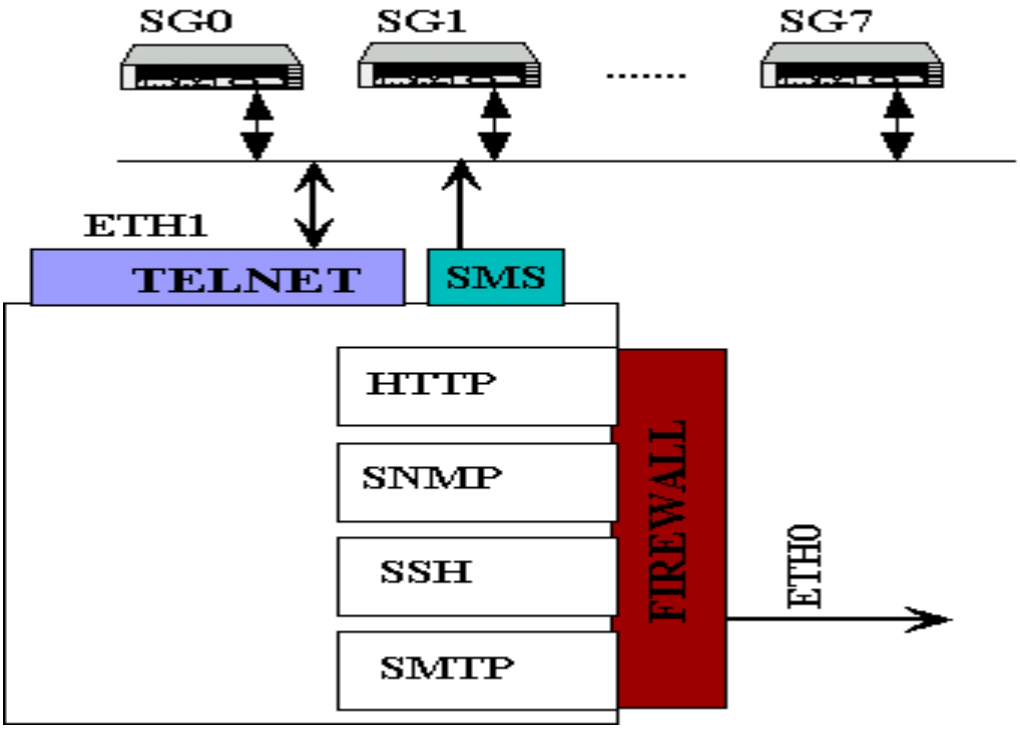

Fig.3: The RCU Protocols

2.1.3 The Management Services Engines

The RCU hosts a total of four management services:

- *Routing Service Engine (RSE)*: Serves for external routing

- *ISDN Trace Service Engine (ITSE)*: This engine is responsible for downloading ISDN traces
- *Status Service Engine (SSE)*: Responsible for periodically downloading statuses of the PRI GSM gateways. If an undesired status is observed, the corresponding status alarm is generated.
- *SMS and E-mail Service Engine (SESE)*: This service can be invoked to send an alarm by either an SMS or e-mail

2.1.4 The Management Databases

- *Status Database (SDB)*: Actual PRI GSM gateway statuses are stored here for each managed PRI GSM gateway. These include databases Stargate0-7
- *ISDN traces, CDR and Log database (IC&LDB)*: Just as the name indicates, this DB stores ISDN traces, Call Data Records and Management application logs for the managed PRI GSM gateways
- *Routing Database (RDB)*: Used by RSE for external routing purposes (see Fig. 4.)
- *Configuration database (CDB)*: This database is used for web configuration, a platform for configuring PRI GSM gateway over the web.

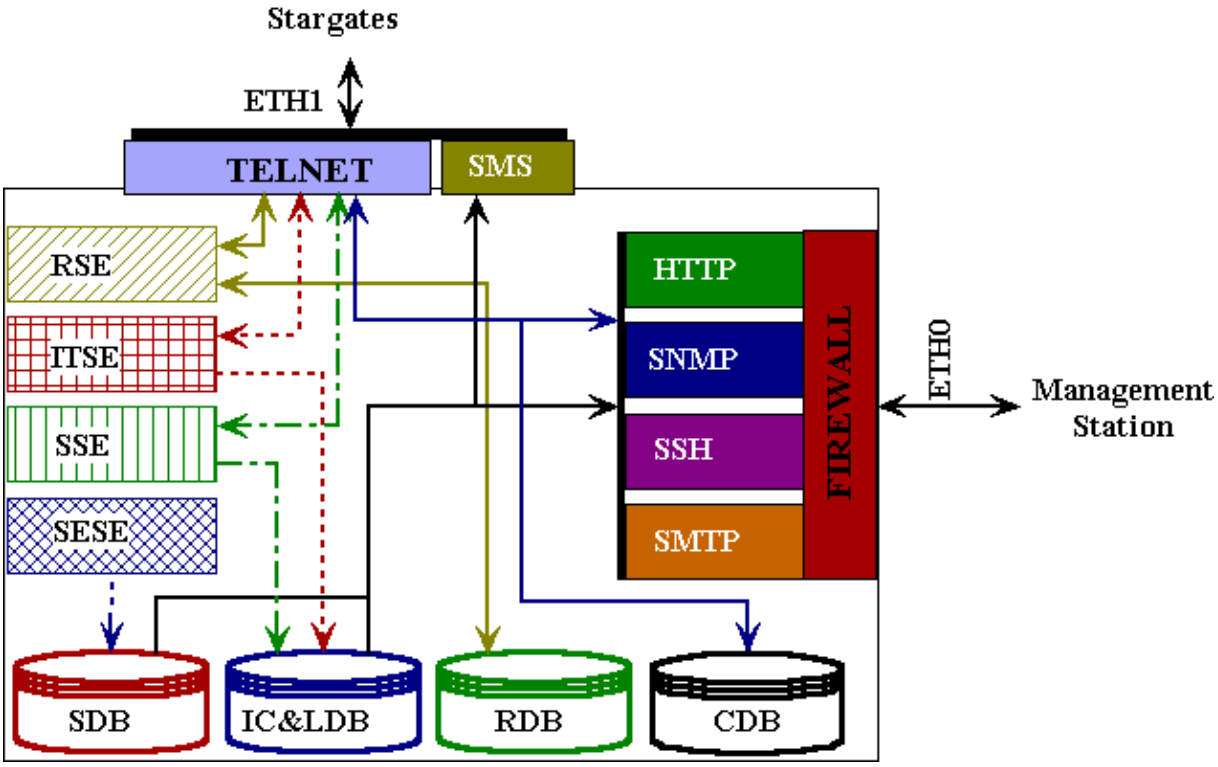

Fig.4: The RCU services and databases

3 Installation

3.1 Pre-installation

For a comprehensive and painless installation, a pre-installation preparation is mandatory.

3.1.1 Topology

The RCU can communicate with PRI GSM gateways in any one of the following modes:

- *RS-232* serial communication through COM1&COM2. This mode can be used if at least one of the PRI GSM gateways is within the proximity of the RCU. It is recommended that this mode be used when only one PRI GSM gateway is to be managed by the RCU
- *Ethernet (10BaseT).* There exists, as many logical network topologies, as there are network technicians. In the following chapter, only those parameters that a technician needs to know in order to either fit in the RCU into an existing network or to come up with a network for this purpose will be presented.

3.1.2 Assigning IP addresses

The RCU demands two logical sub-networks.

- *The PRI GSM gateway sub-network (SG-SUBNET)*: Eth1 of the RCU and all the PRI GSM gateways must belong to the SG-SUBNET. If different PRI GSM gateways are placed in different logical network segments then you may consider implementing Network Address Translation (NAT) so that all the PRI GSM gateways will appear to belong to the same network segment. Majority of network technicians put both Eth1 and the PRI GSM gateways in to a private LAN (10.0.0.0, 192.168.0.0 etc.). The communication protocol in this segment is TELNET.
- *The Management sub-network (MNGMNT-SUBNET)*: Eth0 interface on the RCU is assigned an IP address from this segment. The management station must be reachable from Eth0. If traffic between RCU and the management station goes through a firewall, then, depending on the desired services the following protocols may need to be enabled:

Application protocol	Transport Protocol	Port
HTTPS	TCP	443
SSH	TCP	22
SNMP	UDP	161,162
SMTP	TCP	25

Table1: Protocols to consider allowing through the Firewall

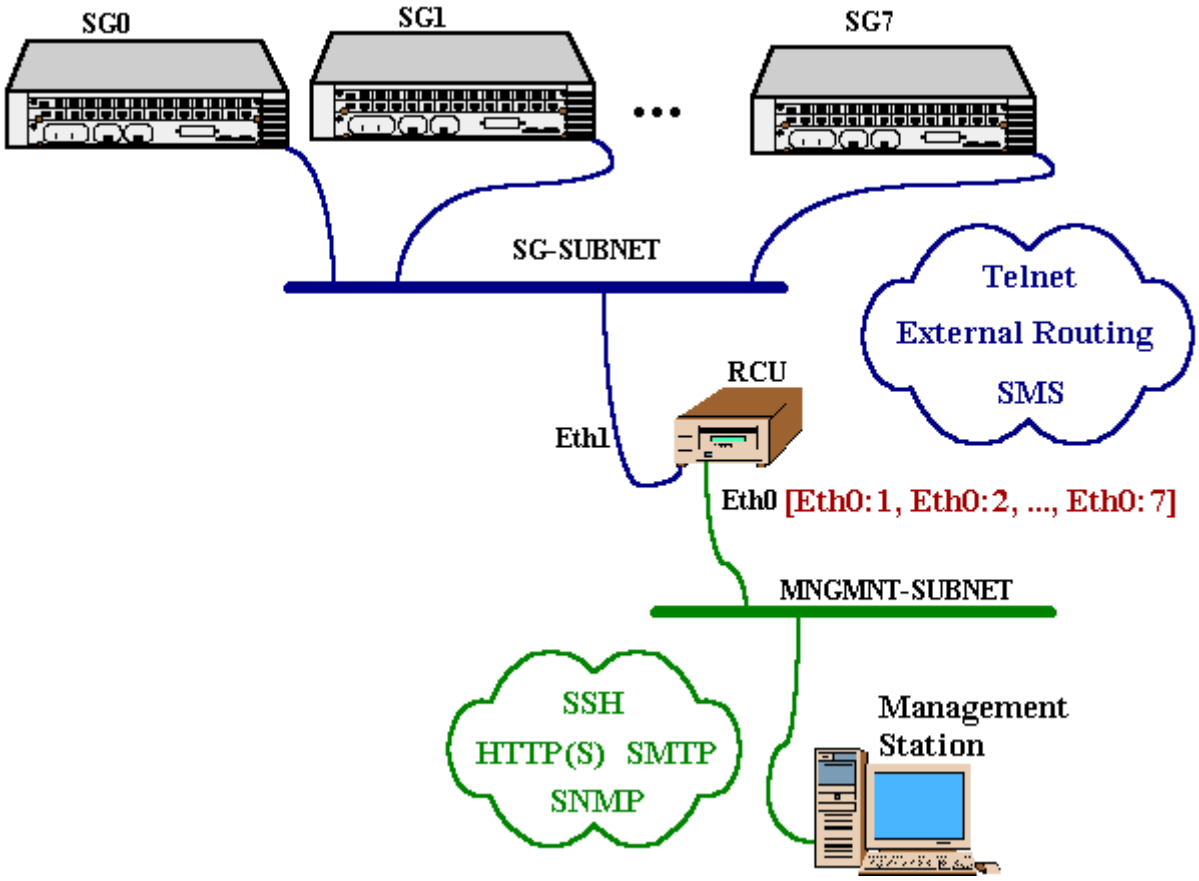

Fig.5: The RCU Topology

For each managed PRI GSM gateway, the RCU runs a separate SNMP agent. Each running SNMP agent requires an IP address to communicate with the SNMP management node. Let us assume that our RCU will proxy eight PRI GSM gateways (SG0, SG1, …, SG7), The SNMP agent for SG0 will use Eth0 to communicate with the SNMP management node. The remaining seven SNMP agents (SG1 – SG7) will need seven additional IP addresses from the MNGMNT-SUBNET. These seven additional IP addresses are added as aliases to Eth0 (Eth0:1, Eth0:2, …, Eth0:7) see Fig.5.

3.2 OS installation

3.2.1 Installation procedure

- Power the RCU
- Insert the RCU-CD into the CD-ROM
- Press Enter to Boot from the CD-ROM when prompted
- Type “y” to format the HD and to go on and install the RCU SW when prompted
- Wait for the system to eject the RCU-CD and press the “Reset” button to reboot the system. If you have gone this far, the OS is installed!
- Stand by for the system to reboot and press any key enter HW configuration. Please pass the screens picking the defaults, this will usually do, alternatively, tweak to taste!
- Type “root“ at the login prompt. “skakal pes pres oves++” is the default password.

4 Configuration

4.1 Basic configuration

Type *sgsetup* at the bash prompt to run the management software configuration script

bash-2.05a#
bash-2.05a# *sgsetup*

The SGSETUP configuration script will guide you through the entire configuration process needed to set up the RCU. The text below will take us through the different options

Enter current date [07.08.2003]:
Today's date

Enter current time [15:01]:
The time now

eth0: IP address [192.168.100.100]:
IP address assigned the Eth0

eth0: Netmask [255.255.255.0]:
Subnet mask for the MNGMNT-SUBNET

eth0: Default gateway [192.168.100.1]:
IP address of the gateway used to reach the network management station (not necessary if the RCU'sEth0 and the management station are in the same network segment)

eth1: IP address [192.168.10.2]:
IP address assigned to Eth1

eth1: Netmask [255.255.255.0]:
Subnet mask for the SG-SUBNET

SNMP trap IP address (1) [192.168.100.3]:
Management stations IP address

SNMP trap IP address (2) [192.168.100.3]:
Backup management station (The same management station can be used for redundancy)

SNMP community [public]:
Every device managed by SNMP must belong to an SNMP community (Public community is the default. The same community name must be set in the management node)

4.1.1 E-mail alarms

Enable e-mail sending? [YES]:
Answer yes (y) to enable e-mail alarms, no (n) disables this option

E-mail 'FROM' address [stargate@2n.cz]:
This entry acts as the sender (source) of the e-mail

E-mail 'TO' address [adminsg@2n.cz]:
You must enter the e-mail address of the PRI GSM gateway monitoring crew here.

E-mail subject [Test]:
The e-mail alarm subject will always be set to this entry.

SMTP server address [10.254.1.254]:
Please be sure to enter your mail server's IP address (DO NOT USE YOUR MAIL SERVER'S HOST NAME, THE RCU DOES NOT USE DNS).

You can select alarms that should be sent by e-mail. That procedure is described in section **Alarm filtering** (4.1.10).

4.1.2 SMS alarms

Enable SMS sending? [YES]:
Answer yes (y) to enable alarm SMSs, no (n) disables this option

Destination phone number [+420737235896]:
SMS recipients GSM phone number

MS Center number [+420603052000]:
The provider's SMS center number. (Note: Provider's SMS center number is currently not implemented, please set a valid SMS center in the selected SIM card.)

SMS0 gateway device number (or type '-' to disable it) [7]:
SMS1 gateway device number (or type '-' to disable it) [-]:
SMS2 gateway device number (or type '-' to disable it) [-]:
The PRI GSM gateway through which the SMS alarm is sent (one of 0 - 7 managed PRI GSM gateways). Up to three different PRI GSM gateways can be used for this purpose. Typing "–" disables the particular choice.

SMS0 module number [2]:
SMS1 module number [2]:
SMS2 module number [2]:
The GSM module from which the SMS alarm is sent, Three GSM modules can be set, they must belong to the PRI GSM gateways selected above.

You can select alarms that should be sent as SMS messages. The procedure is described in section **Alarm filtering** (4.1.10)

4.1.3 Call Data Records (billing)

The RCU collects Call Data Records (CDR) that contains all important information about each call that has passed through PRI GSM gateway. These data could be used for billing purposes. Configuration procedure in sgsetup gives you possibility to enable or disable this collection for each managed gateway. It is enabled by default, but there are some situation when it should be disabled. For instance, **it must be disabled if the gateway at the same time uses the SMS Callback Centrum application i.e. you must write *Y* in that case.**

Disable billing from Gateway #0 ? [NO]:

You can find more details about CDR in chapter **5.3 Accounting** and in your gateway documentation.

4.1.4 The ASR statistics

The Answer to Seizure Ratio (ASR) is a statistical parameter used to express call success rate in world of voice communications. Vendors of the related equipment use various definitions of ASR. The RCU gives possibility to choose between two definitions. The following values should be calculated for each SIM card, every 5 minutes according to calls made in that time interval.

1. [Δ(successfull calls) / Δsuccessfull calls + calls rejected by gateway + calls rejected by GSM)] x 100

or

2. [Δ(successfull calls) / Δsuccessfull calls + calls rejected by gateway + calls rejected by GSM + calls dropped by calling party)] x 100

Answer to the following question (from sgsetup) decides which of two should be used

Calls dropped by calling party counted in ASR? [YES]:

If you answer N, the first formula is used. In other case, the second one. The calculated values are presented through Web in SIM Card Statistics.

Two alarms(traps) are introduced in RCU ver. 2.0 to signalize important changes of ASR. The first one (specific number 555) is sent when ASR falls under value defined as Low ASR. The second one is sent when ASR is improved over value defined as Good ASR. These values are set as response on the following sgsetup question

Low ASR [70]:
Good ASR [80]:

4.1.5 Utilization of PRI ports

The RCU checks every minute number of busy(active) B channels on both PRI ports. This information is used to generate four traps related to high and low picks of traffic.

B channel high_up limit[29]:

B channel high_down limit[28]:

Trap 529 is sent when number of busy channels improves to value over high_up limit, and trap 530 is sent when this value falls under high_down limit.

B channel low_down limit[3]:
B channel low_up limit[5]:

Trap 531 is sent when number of busy channels falls to value under low_down limit, and trap 532 is sent this number improves over low_up limit.

4.1.6 The PRI GSM gateways

At this stage, we configure the PRI GSM gateways to be managed by the RCU. For each PRI GSM gateway, five parameters have to be configured as shown below. These five items have to be repeatedly configured a number of times equal to the number of PRI GSM gateways. The PRI GSM gateways are numbered from zero, so that, if for example we have eight PRI GSM gateways, they will be numbered from 0 through 7. This same order will be used to map the PRI GSM gateways to the different databases and storage tables. It is therefore mandatory to maintain the same PRI GSM gateway numbering as the one that comes with the RCU CD.

ATTENTION: SWAPPING CPU CARDS BETWEEN PRI GSM GATEWAYS IS NOT POSSIBLE BECAUSE INDIVIDUAL PRI GSM GATEWAYS ARE BOUND TO THEIR DATABASES BY THE SERIAL NUMBERS OF THEIR CPUs!
THE RCU HAS BEEN TESTED TO WORK RELIABLY WITH UP TO EIGHT PRI GSM GATEWAYS. MORE THAN EIGHT PRI GSM GATEWAYS CAN ONLY BE CONFIGURED AT USER'S RISK.

Enable Gateway #0 ? [YES]:
Enter yes (y) to enable the first Gateway. If SNMP will be used to manage this Gateway then it will be automatically bound to Eth0. No (n) disables Gateway #0

Enable Gateway LCR #0 ? [YES]:
Yes (y) switches on External Routing, No (n) turns it off

Enter Gateway #0 IP address or '-' [192.168.10.3]:
This parameter has a number of meanings. The first is that we choose the mode of communication. By entering „-"(dash) we tell the RCU that it will communicate with PRI GSM Gateway #0 through the serial ports (COM1 and COM2). Make sure that PRI GSM Gateway #0 is connected to the RCU by serial cables (PRI GSM Gateway COM1 to RCU COM1 and PRI GSM Gateway COM2 to RCU COM 2). Only one PRI GSM Gateway can use this form of communication. If however, the RCU will use Ethernet to communicate with PRI GSM Gateway #0 then this is the right place to enter PRI GSM Gateway #0's IP address.

Enter Gateway #0 user name [2n]:
Enter Gateway #0 user password [2n]:
If Ethernet is enabled as above, it is mandatory to configure username and password. The username and password entered here must be the same as the username and password configured in the PRI GSM Gateway, it will otherwise reject telnet sessions from the RCU.

(Username and password are case sensitive!)

These same parameters must be repeatedly set for all the PRI GSM Gateways managed by the RCU (#1 through #7). See the Example configuration in the next section.

4.1.7 Network Address Translation

A classical Network Address Translation (NAT) is applied here to map the SNMP IP addresses configured on Eth0 (Eth0, Eth0:1, … Eth0:7) to the IP addresses of the PRI GSM Gateways usually reachable from Eth1. This parameter can be safely turned off if SNMP will not be used for management.

Enable network address translation? [YES]:
Yes (y) turns on NAT, no (n) turns it off

4.1.8 SNMP Configuration

IP address of SNMP agent #0: 192.168.20.100
Each managed PRI GSM Gateway has a separate SNMP agent whose task is to proxy the specific PRI GSM Gateway to the network management node. Each of these SNMP agents uses the IP addresses set on Eth0. See table below.

Interface	Agent	Gateway
Eth0	agent #0	Gateway #0
Eth0:1	agent #1	Gateway #1
Eth0:2	agent #2	Gateway #2
.	.	.
.	.	.
Eth0:n	agent #n	Gateway #n

Table2: Interface, SNMP agent and PRI GSM Gateway Mapping

Gateway #0 is automatically bound to Eth0, which is already configured. Gateways #1 through n have to be manually assigned SNMP IP addresses, these are the IP addresses made for Eth0:1 through Eth0:n, n is the number of Gateways to be managed by the RCU minus 1, the maximum value n can take is 7.

4.1.9 Binding PRI GSM Gateways to databases

PRI GSM Gateway CPUs are usually bound to the RCU databases before shipping. In this case no additional binding is required. It may happen however, that the RCU and the PRI GSM Gateways are shipped separately or that a customer decides to buy additional PRI GSM Gateways and therefore pre-shipment binding is not done. This subsection is devoted to binding PRI GSM Gateway CPUs to the RCU databases when this becomes necessary.
For each PRI GSM Gateway CPU that has not already been bound to a database in the RCU, 3 key codes are provided in the acompaning letter received with the RCU , Please prepare these codes for each PRI GSM Gateway and follow the procedure below.

- Run “chcpusn”

bash-2.05a#
bash-2.05a# chcpusn

Enter number of database (0 7)
Pick a database for this PRI GSM Gateway, it must be free (not previously allocated to another one).

Enter 1. string:
Enter the first key code for this PRI GSM Gateway

Enter 2. string:
Enter the second key code for this PRI GSM Gateway

Enter 3. string:
Enter the third key code for this PRI GSM Gateway

- Test database to PRI GSM Gateway CPU binding

bash-2.05a#
bash-2.05a# sgterm n "ati4"

The output of this AT command is the CPU serial number of the PRI GSM Gateway bound to database number n (If we chose 5 in ***Enter number of database (0 7)*** above, then use 'sgterm 5 "ati4"' to retrieve the CPU serial number for the database Stargate5 and compare it with the one given in the acompaning letter).

4.1.10 External routing

Before external routing can be activated, the RCU has to be prepared for this. Please follow the following steps to prepare the RCU for external routing.

- Edit the text file */var/local/stargate/routing_list.txt*. This file comes with a default configuration, which is usually not usable; please edit this file so that the first column contains the list of dialed numbers. The second column must contain the target groups through which the PRI GSM Gateway will route the calls. Use groups 1-8 for calls that will be routed. Numbers that will be blocked should have 0 in the second column. Be sure to follow the format in the default file.
- Run "sgrt"

bash-2.05a#
bash-2.05a# sgrt
This script uploads the contents of *routing_list.txt* in to the appropriate tables in the routing database. Any duplicate entries are removed during this operation. Before you consider using external routing, make sure you have a fast Ethernet connection between the PRI GSM Gateway and the RCU.

4.1.11 Alarm filtering

Alarms (traps) sent by RCU could be divided, according to the severity of the reason that provoked them, in four categories:

- critical
- major
- minor
- warning

All alarms with an advice of severity level are contained in **The Trap Table** (Appendix 1).

You can choose which alarms should be sent as SMS message and/or e-mail (if enabled in sgsetup!). For this purpose is used file /etc/stargate-traps.conf, where is possible to give severity level to each alarm(trap) and define sending rules for each severity level. Here we have an example of its content.

```
501=warning
502=warning
503=critical
504=major
505=minor
511=major
512=minor
555=critical
556=warning

critical=sms,mail
major=sms,mail
minor=mail
warning=mail
```

The first part is a list of trap specific numbers (see. Appendix 1) with attached severity levels. They could corespond to the advised ones in the Appendix 1, but also could be configured due to users criteria. Traps not mentioned in the list will not be sent as SMS or e-mail at all. The second part defines rules of sending SMS and e-mails dependant on the severity level. You can configure it according to your needs.

4.2 Web access configuration

All the PRI GSM Gateways are now available on the web. Only authorized users can however access this information. To be able to access the individual PRI GSM Gateways over the web, we will need to create a web username and password for each managed unit. You are advised to set the same username and password for all the PRI GSM Gateways to avoid errors during automatic actualization.

bash-2.05a#
At the bash prompt, type ‘webpass’ to invoke the web password configuration script

bash-2.05a# webpass
Gateway num.:
Enter the PRI GSM Gateway Number (0 through n)

Username:
New password:
Re-type new password:
The username and password for the PRI GSM Gateway number set above.

This procedure has to be repeated n times to have all n gateways accessible over the web.

4.3 Testing

The first thing to do after configuration is to restart the PRI GSM Gateways services. This forces them to re-read the current configuration files.

bash-2.05a#
bash-2.05a# service stargate restart

To troubleshoot the stargate service use the commands ”service stargate status “ and „sgconf“ for further information, see the example in the next section.

4.4 Configuration Example

Refer to Fig. 6

4.4.1 IP map Table

PRI GSM Gateway	PRI GSM Gateway IP address	Interface	Interface IP address	Interface Use
SG0	192.168.10.2	Eth0	192.168.20.2	SNMP SG0, SSH, SMTP, HTTPS
SG1	192.168.10.3	Eth0:1	192.168.20.3	SNMP SG1
SG2	192.168.10.4	Eth0:2	192.168.20.4	SNMP SG2
SG3	192.168.10.5	Eth0:3	192.168.20.5	SNMP SG3
SG4	192.168.10.6	Eth0:4	192.168.20.6	SNMP SG4
SG5	192.168.10.7	Eth0:5	192.168.20.7	SNMP SG5
SG6	192.168.10.8	Eth0:6	192.168.20.8	SNMP SG6
SG7	192.168.10.9	Eth0:7	192.168.20.9	SNMP SG7
		Eth1	192.168.10.1	Telnet, HTTPS, SMS

Table3: IP address and protocol plan

Default gateway 192.168.20.1, Management Station 192.168.30.5

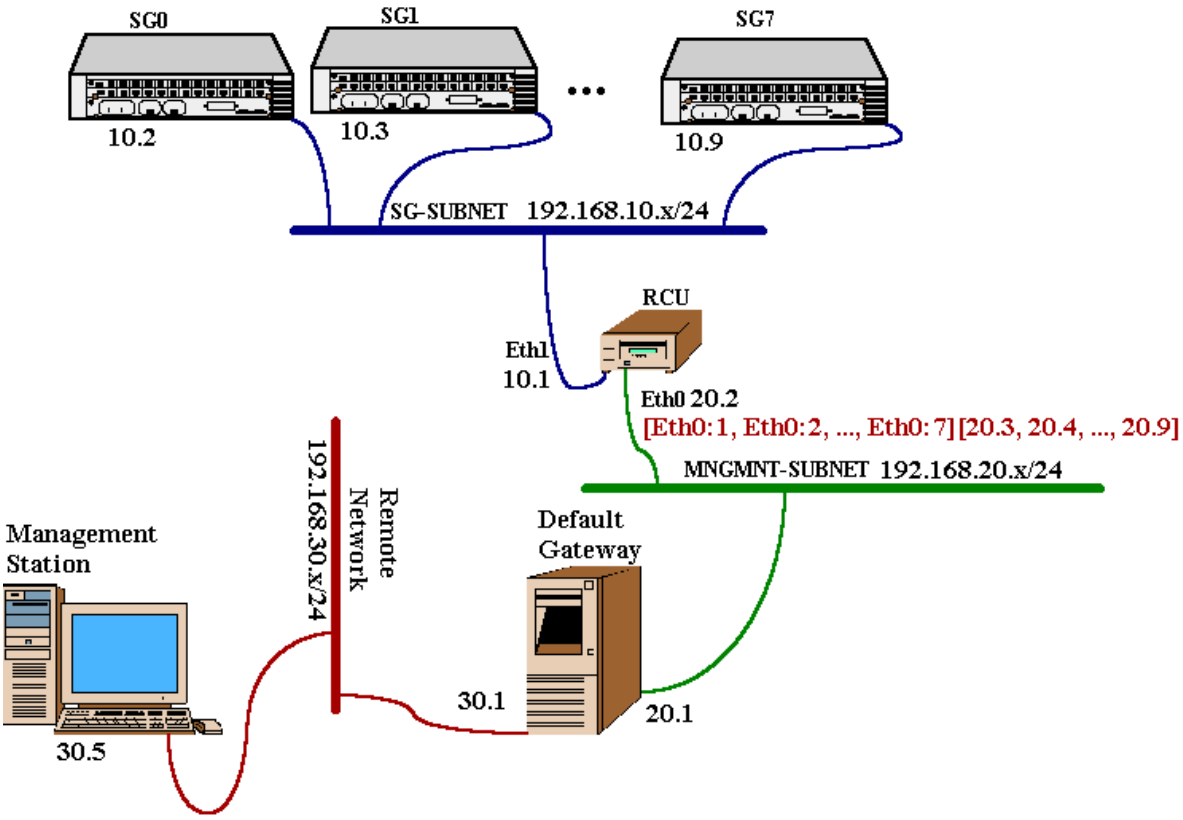

Fig. 6: An example configuration.

4.4.2 Configuration

bash-2.05a#
bash-2.05a# *sgsetup*
Enter current date [07.08.2003]: *09.08.2003*

Sat Aug 9 00:00:00 CEST 2003

Enter current time [15:01]: *21.33*

Sat Aug 9 21:33:00 CEST 2003
Date and time are updated.

eth0: IP address [192.168.100.100]:192.168.20.2
eth0: Netmask [255.255.255.0]: *255.255.255.0*
eth0: Default gateway [192.168.100.1]: *192.168.20.1*

eth1: IP address [192.168.10.2]: *192.168.10.1*
eth1: Netmask [255.255.255.0]: *255.255.255.0*

SNMP trap IP address (1) [192.168.100.3]: *192.168.30.5*
SNMP trap IP address (2) [192.168.100.3]: *192.168.30.5*
SNMP community [public]: *Buster*

Configuring network interface eth0 ...
Configuring network interface eth1 ...

Enable e-mail sending ? [YES]: *y*
E-mail 'FROM' address [stargate@2n.cz]: *remote-tower@control-center.com*
E-mail 'TO' address [ryba@2n.cz]: *watch-tower@control-center.com*
E-mail subject [Test]: *Stargate watch*

SMTP server address [10.254.1.254]:192.168.30.2

Enable SMS sending ? [YES]: y
Destination phone number [+420737235896]: +420900333777
SMS Center number [+420603052000]: +420900600000
SMS0 gateway device number (or type '-' to disable it) [7]:1
SMS0 module number [2]: 3
SMS1 gateway device number (or type '-' to disable it) [-]:3
SMS1 module number [2]: 5
SMS2 gateway device number (or type '-' to disable it) [-]:5
SMS2 module number [2]: 7

Calls dropped by calling party counted in ASR? [YES]:
Low ASR [70]:
Good ASR [80]:

B channel high_up limit[29]:
B channel high_down limit[28]:
B channel low_down limit[3]:
B channel low_up limit[5]:

Disable billing from Gateway #0 ? [NO]:
Disable billing from Gateway #1 ? [NO]:
Disable billing from Gateway #2 ? [NO]:
Disable billing from Gateway #3 ? [NO]:
Disable billing from Gateway #4 ? [NO]:
Disable billing from Gateway #5 ? [NO]:
Disable billing from Gateway #6 ? [NO]:
Disable billing from Gateway #7 ? [NO]:

Enable Gateway #0 ? [YES]: y
Enable Gateway LCR #0 ? [YES]:n
Enter Gateway #0 IP address or '-' [192.168.10.3]:192.168.10.2
Enter Gateway #0 user name [2n]: spinner
Enter Gateway #0 user password [2n]: secrets

Enable Gateway #1 ? [YES]: y
Enable Gateway LCR #1 ? [YES]:n
Enter Gateway #1 IP address or '-' [192.168.10.10]:192.168.10.3
Enter Gateway #1 user name [2n]: spinner
Enter Gateway #1 user password [2n]: secrets

Enable Gateway #2 ? [YES]: y
Enable Gateway LCR #2 ? [YES]:n
Enter Gateway #2 IP address or '-' [192.168.10.6]:192.168.10.4
Enter Gateway #2 user name [2n]: spinner
Enter Gateway #2 user password [2n]: secrets

Enable Gateway #3 ? [YES]: y
Enable Gateway LCR #3 ? [YES]:n
Enter Gateway #3 IP address or '-' [192.168.10.7]:192.168.10.5
Enter Gateway #3 user name [2n]: spinner
Enter Gateway #3 user password [2n]: secrets

Enable Gateway #4 ? [YES]: y
Enable Gateway LCR #4 ? [YES]:n
Enter Gateway #4 IP address or '-' [192.168.10.7]:192.168.10.6
Enter Gateway #4 user name [2n]: spinner
Enter Gateway #4 user password [2n]: secrets

Enable Gateway #5 ? [YES]: y
Enable Gateway LCR #5 ? [YES]:n
Enter Gateway #5 IP address or '-' [192.168.10.7]:192.168.10.7
Enter Gateway #5 user name [2n]: spinner
Enter Gateway #5 user password [2n]: secrets

Enable Gateway #6 ? [YES]: y
Enable Gateway LCR #6 ? [YES]:n
Enter Gateway #6 IP address or '-' [192.168.10.7]:192.168.10.8
Enter Gateway #6 user name [2n]: spinner
Enter Gateway #6 user password [2n]: secrets

Enable Gateway #7 ? [YES]: y
Enable Gateway LCR #7 ? [YES]:n
Enter Gateway #7 IP address or '-' [192.168.10.7]:192.168.10.9
Enter Gateway #7 user name [2n]: spinner
Enter Gateway #7 user password [2n]: secrets

Enable network address translation ? [YES]: y

IP address of SNMP agent #0: 192.168.20.2
IP address of SNMP agent #1 [192.168.100.101]:192.168.20.3
IP address of SNMP agent #2 [192.168.100.102]: 192.168.20.4
IP address of SNMP agent #3 [192.168.100.103]: 192.168.20.5
IP address of SNMP agent #4 [192.168.100.104]: 192.168.20.6
IP address of SNMP agent #5 [192.168.100.105]: 192.168.20.7
IP address of SNMP agent #6 [192.168.100.106]: 192.168.20.8
IP address of SNMP agent #7 [192.168.100.107]: 192.168.20.9

Configuring network interface eth0:1 ...
Configuring network interface eth0:2 ...
Configuring network interface eth0:3 ...
Configuring network interface eth0:4 ...
Configuring network interface eth0:5 ...
Configuring network interface eth0:6 ...
Configuring network interface eth0:7 ...
Setting firewall...
Saving new firewall configuration...
Finished.
bash-2.05a#

4.4.3 Web pass

bash-2.05a#
bash-2.05a# webpass
Gateway num.:0
Username:stargateguru
New password: topsecret
Re-type new password: topsecret

Updating password for user stargateguru

bash-2.05a#
bash-2.05a# webpass
Gateway num.:1
Username: stargateguru
New password: topcecret
Re-type new password: topsecret

Updating password for user stargateguru

etc

4.4.4 Starting

bash-2.05a#
bash-2.05a# service stargate restart

Shutting down StarGate SNMP daemon: [OK]
Shutting down StarGate Agent: [OK]
Shutting down StarGate Trace Logger: [OK]
Shutting down StarGate Least Cost Routing: [FAILED]
Shutting down StarGate Network Server: [OK]
Starting StarGate SNMP daemon #0 [OK]
Starting StarGate Network Server #0 [OK]
Starting StarGate Agent #0 [OK]
Starting StarGate Trace Logger #0 [OK]
Starting StarGate SNMP daemon #1 [OK]
Starting StarGate Network Server #1 [OK]
Starting StarGate Agent #1 [OK]
Starting StarGate Trace Logger #2 [OK]
Starting StarGate SNMP daemon #2 [OK]
Starting StarGate Network Server #2 [OK]
Starting StarGate Agent #2 [OK]
Starting StarGate Trace Logger #2 [OK]
Starting StarGate SNMP daemon #3 [OK]
Starting StarGate Network Server #3 [OK]
Starting StarGate Agent #3 [OK]
Starting StarGate Trace Logger #3 [OK]

4.4.5 Testing

bash-2.05a#
bash-2.05a# service stargate status

snmpd (pid 16705 16645) is running...
sgagent (pid 16734 16671) is running...
sgtrace (pid 16746 16682) is running...
sglcr is stopped
sgethsvr (pid 16722 16660) is running...

bash-2.05a#
bash-2.05a# sgconf

Gateway #0: YES - 192.168.10.2
Gateway #1: YES - 192.168.10.3
Gateway #2: YES - 192.168.10.4
Gateway #3: YES - 192.168.10.5
Gateway #4: YES - 192.168.10.6
Gateway #5: YES - 192.168.10.7
Gateway #6: YES - 192.168.10.8
Gateway #7: YES - 192.168.10.9
Gateway #8: NO
Gateway #9: NO

startage 0: OK
startage 1: OK
startage 2: OK
startage 3: OK
startage 4: OK

startage 5: OK
startage 6: OK
startage 7: OK
startage 8: DISABLED
startage 9: DISABLED

5 RCU Usage

The RCU can be used in a number of ways as has already been explained in the previous chapters. In the following sections, we will explore methods of retrieving and interpreting the management and accounting data gathered by the RCU.

5.1 Web access

To access the managed gateways over the web, open your favorite web browser and for the URL type https://IPaddress. If, as in our example, the IP address of Eth0 is 192.168.20.2, then the URL would be https://192.168.20.2. Note that the IP address can be any one of Eth0, Eth1 or any of the aliases depending on the reachability of the RCU from the control station.

IMPORTANT!!!

For Web access, in RCU ver. 2.0, or higher, you have to use HTTPS!

5.1.1 Welcome Message

The first page that comes up contains a list of the eight manageable PRI GSM gateways (0-7). Active are only gateways that haven't icon N/A on the left side.
The button column 'Web Overview' is used to select the gateway.
Clicking on any of the buttons will take us to a login dialogue if we are not already logged in (see Fig. 7&8).

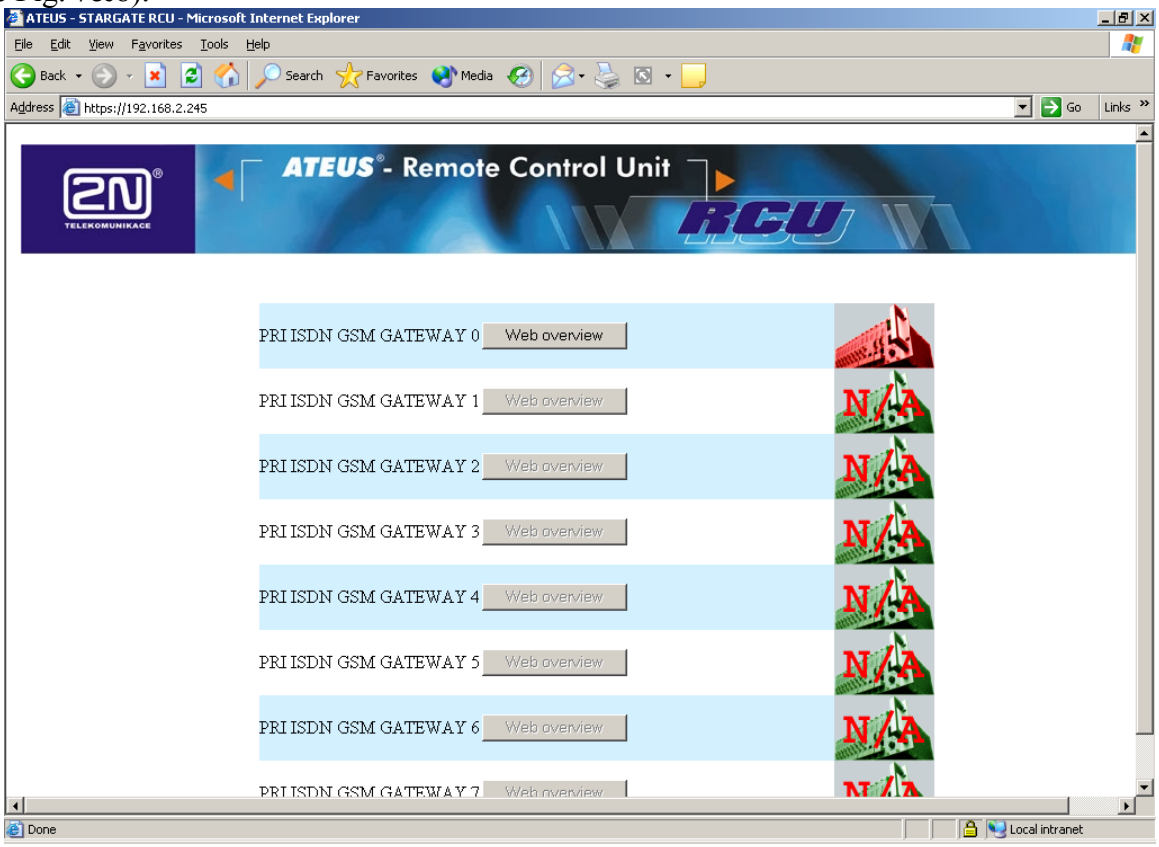
ATEUS - STARGATE RCU - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.2.245
Go Links
ATEUS - Remote Control Unit
RCU
PRI ISDN GSM GATEWAY 0 Web overview
PRI ISDN GSM GATEWAY 1 Web overview
PRI ISDN GSM GATEWAY 2 Web overview
PRI ISDN GSM GATEWAY 3 Web overview
PRI ISDN GSM GATEWAY 4 Web overview
PRI ISDN GSM GATEWAY 5 Web overview
PRI ISDN GSM GATEWAY 6 Web overview
N/A
Done
Local intranet

Fig.7: Web access welcome page

5.1.2 Authentication

Here, it is enough to type the username and password configured in the RCU with the ‘webpass’ command. Let us visit the ‘Web Overview’ first (Fig.9).

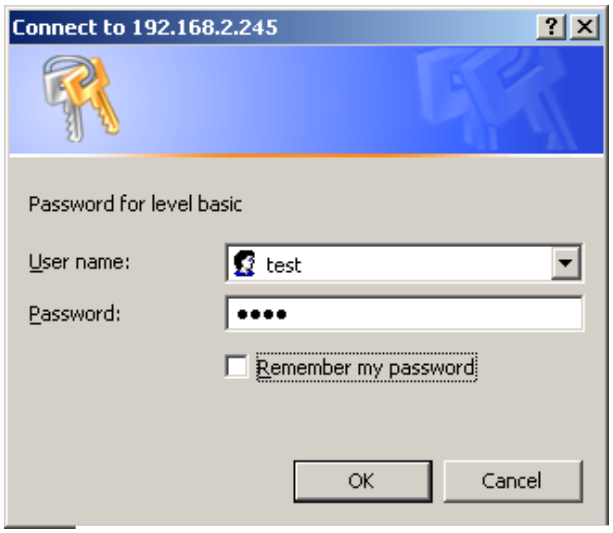

Fig.8: Web login dialogue

5.1.3 Web Overview

The Web Overview is the main management page as can be seen in the Fig.9. In the center is

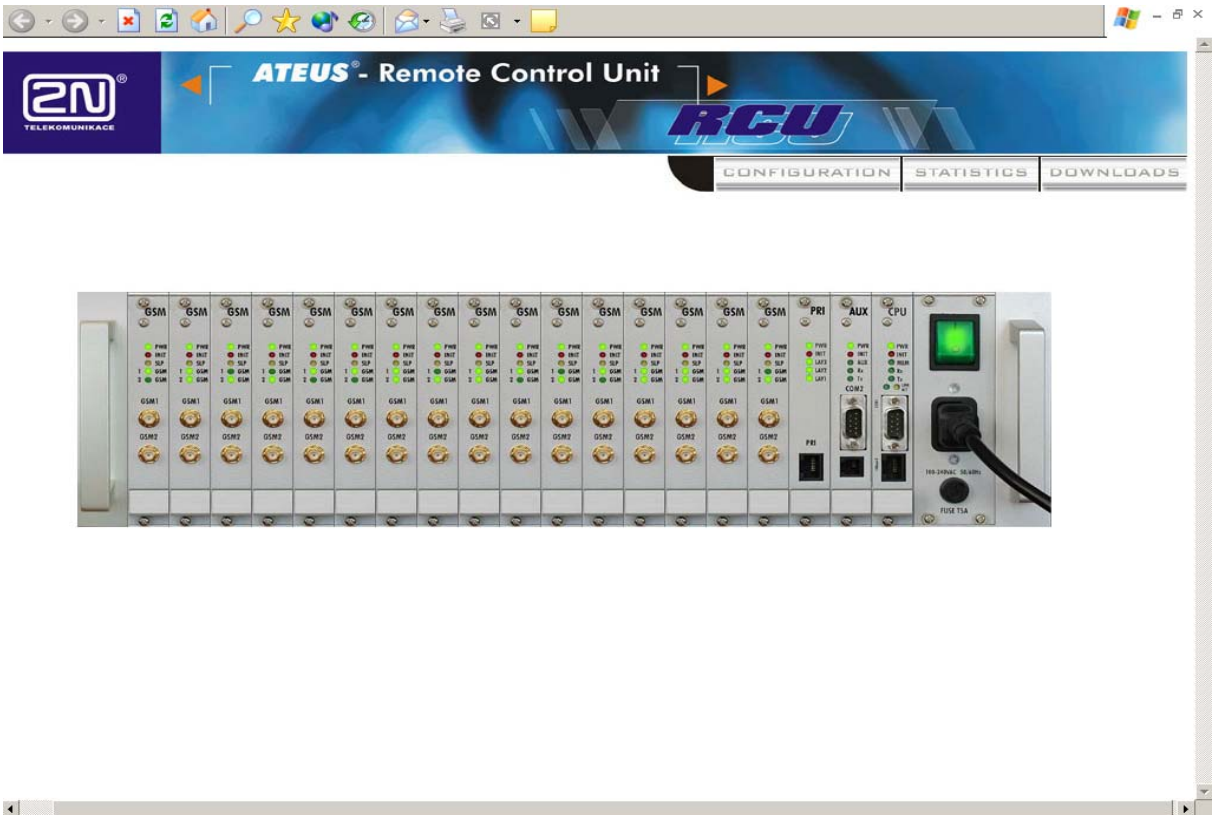

Fig.9: Web Overview

the front view of the PRI GSM gateway. Counting from right, we have the power supply, the CPU card, the AUX card, the PRI card and 16 GSM cards (In case of Bluestar only 8 of them could be active). When something happens to any of the cards, the card color changes from gray to red. If we however put one of the GSM modules to 'sleep' or 'block' mode, the corresponding card turns yellow (Fig. 10). This page refreshes automatically every 20 seconds so that any faults investing the PRI GSM gateway are diagnosed in 20 seconds latest. Please consult the PRI GSM gateway manual for more information. Clicking on the CPU card you can get the System Settings as configured with the Stargate or Bluestar program.

On the upper part are three buttons. The left most button opens the web configuration page (Fig.13). Click the middle button to display call statistics (Fig.11). The right most button is used for downloading CDRs and ISDN PRI traces (Fig.12).

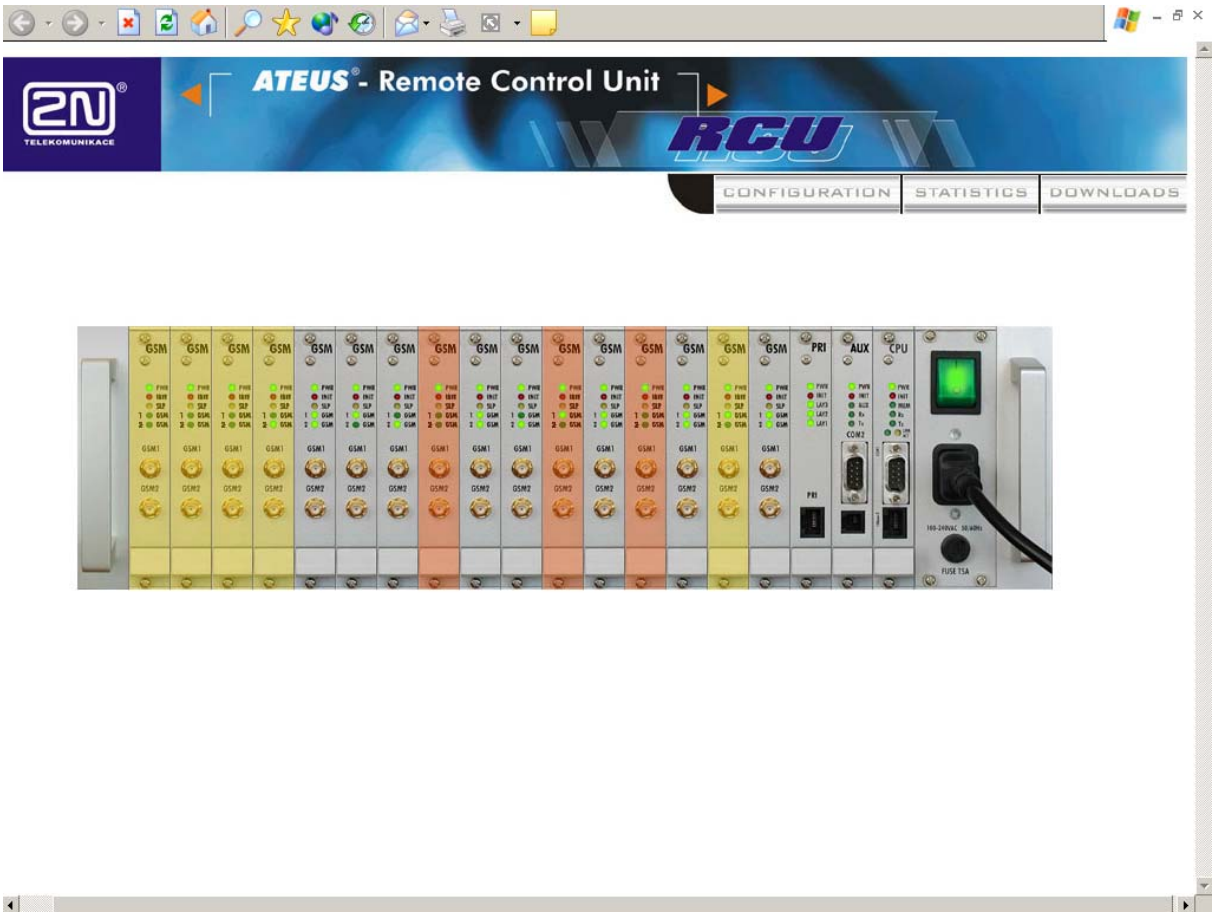

Fig.10: Error conditions

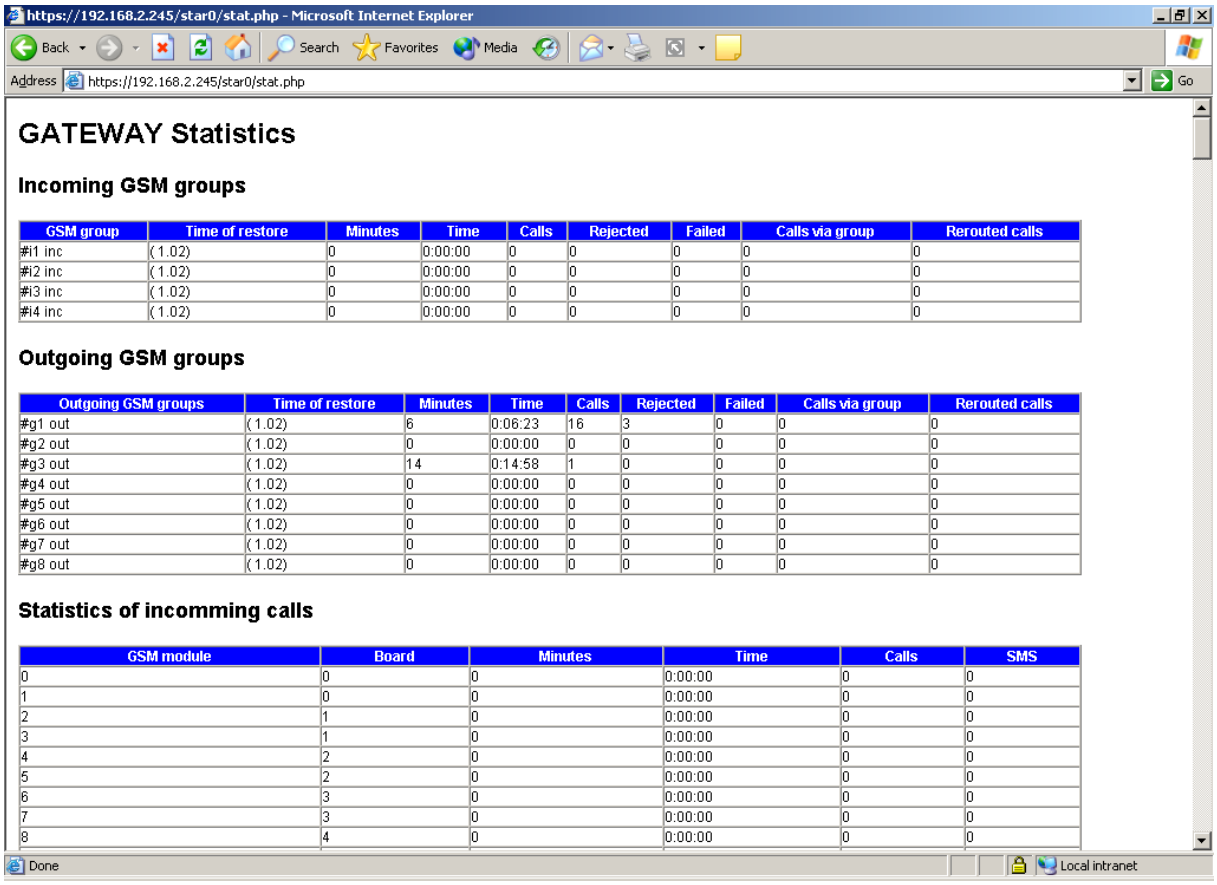
https://192.168.2.245/star0/stat.php - Microsoft Internet Explorer
Back
Search
Favorites
Media
Address
https://192.168.2.245/star0/stat.php
Go
GATEWAY Statistics
Incoming GSM groups
GSM group | Time of restore | Minutes | Time | Calls | Rejected | Failed | Calls via group | Rerouted calls
#i1 inc | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#i2 inc | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#i3 inc | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#i4 inc | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
Outgoing GSM groups
Outgoing GSM groups | Time of restore | Minutes | Time | Calls | Rejected | Failed | Calls via group | Rerouted calls
#g1 out | (1.02) | 6 | 0:06:23 | 16 | 3 | 0 | 0 | 0
#g2 out | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#g3 out | (1.02) | 14 | 0:14:58 | 1 | 0 | 0 | 0 | 0
#g4 out | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#g5 out | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#g6 out | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#g7 out | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
#g8 out | (1.02) | 0 | 0:00:00 | 0 | 0 | 0 | 0 | 0
Statistics of incomming calls
GSM module | Board | Minutes | Time | Calls | SMS
0 | 0 | 0 | 0:00:00 | 0 | 0
1 | 0 | 0 | 0:00:00 | 0 | 0
2 | 1 | 0 | 0:00:00 | 0 | 0
3 | 1 | 0 | 0:00:00 | 0 | 0
4 | 2 | 0 | 0:00:00 | 0 | 0
5 | 2 | 0 | 0:00:00 | 0 | 0
6 | 3 | 0 | 0:00:00 | 0 | 0
7 | 3 | 0 | 0:00:00 | 0 | 0
8 | 4 | 0 | 0:00:00 | 0 | 0
Done
Local intranet

Fig.11: PRI GSM gateway statistics

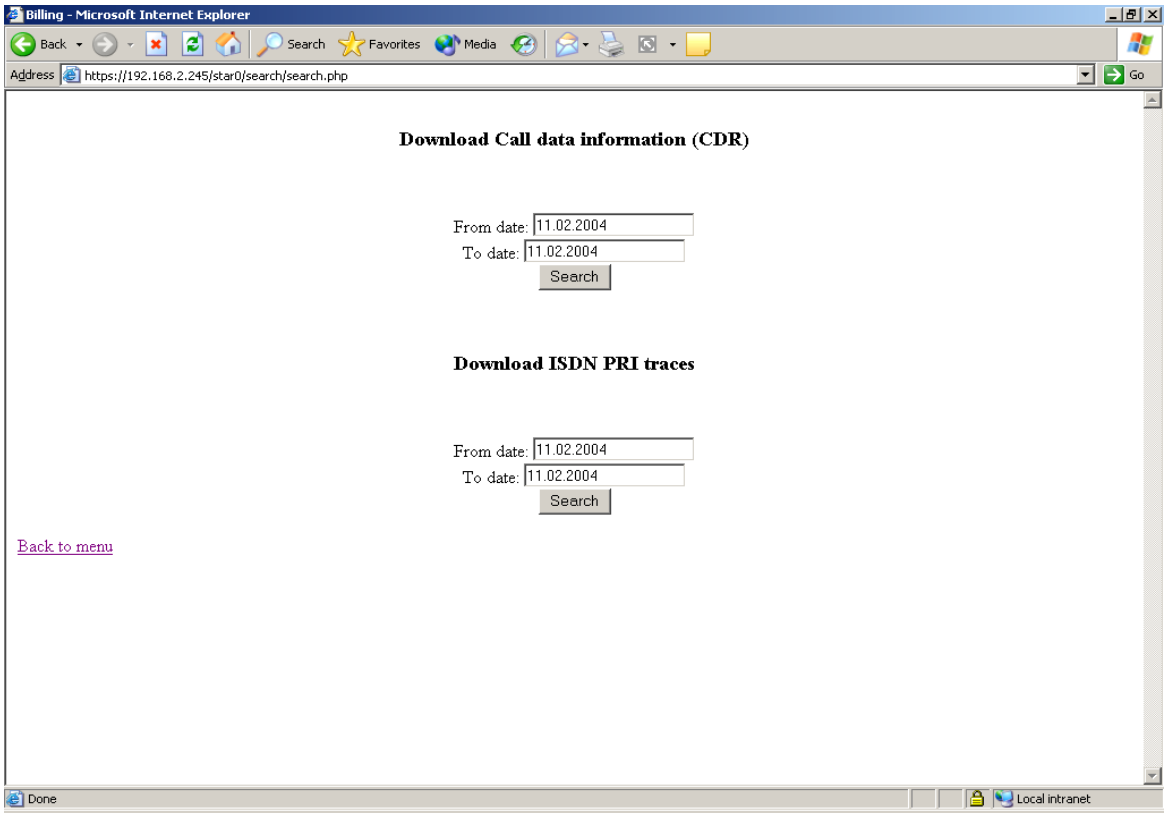

Fig.12: CDR and Trace download

5.1.4 Web configuration of the gateway

This item, which is recommended only for trained technicians, is intended for the configuration of the PRI GSM gateway over the web. If you are not sure of what you are doing please do not use this page. You can configure PRI GSM gateway the same way as it could be done by Stargate(Bluestar, Bluetower) program.

To modify the PRI GSM gateway configuration through the web interface, please follow these 3 simple steps

- Make the desired changes on the web interface
- Click “Save settings” on the page where changes has be done, to send the changes to the database in the RCU
- Click “Upload data in the gateway” (red arrow) on the first page, to load the settings from the database into the PRI GSM gateway.

Please note that the second step have to be repeated on each page.

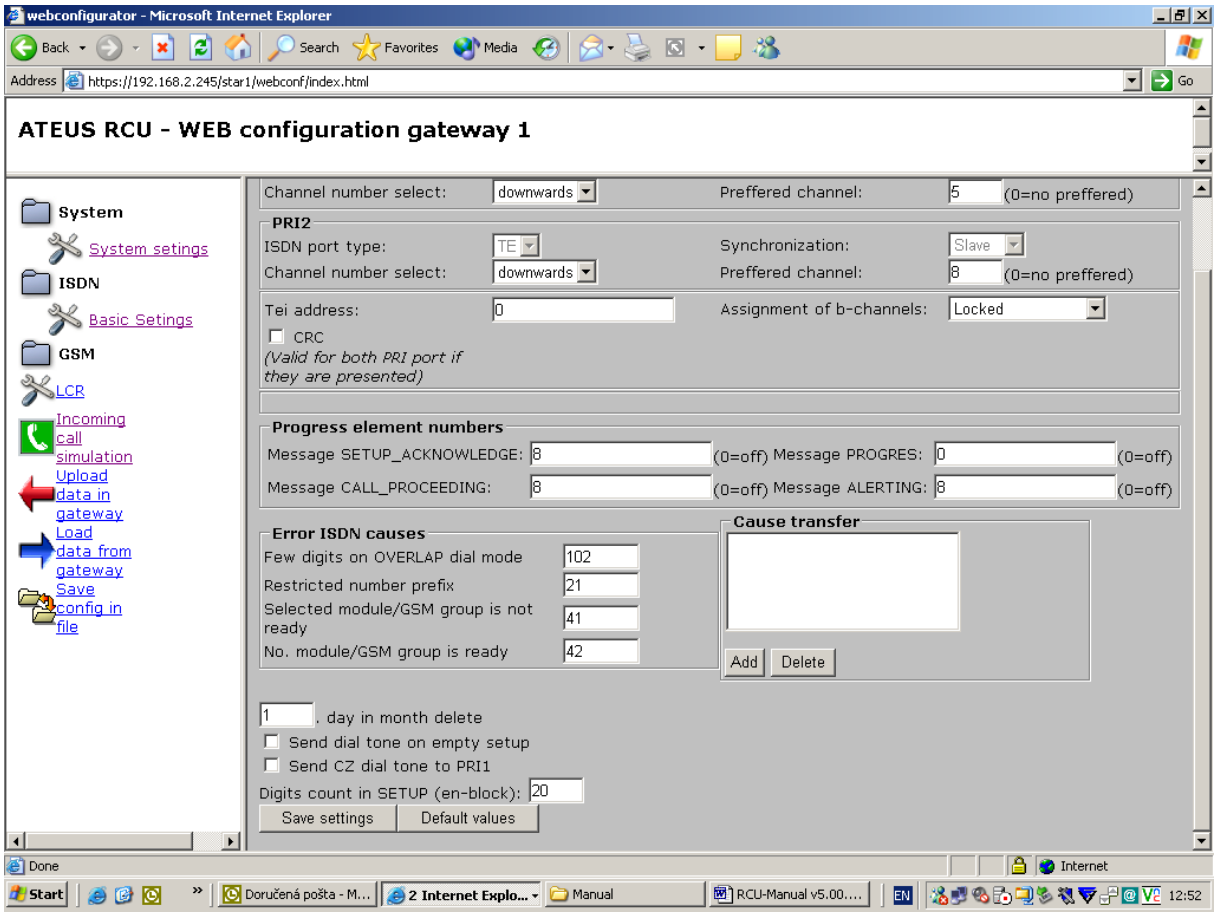

Fig.13: Web configuration

5.1.5 Incomming Call Simulation

New function implemented in the version 4.00 of the RCU is Incoming Call Simulation (ICS). This function provides to generation of the fake calls to SIM cards in the gateway, avoiding easy visible zero incomming traffic on these cards. You can start configuration of this

function through the main Web configuration menu (Fig.13). It is possible to define for each SIM card, whether it should be called or not. You can also define calling frequency (Fig. 14).

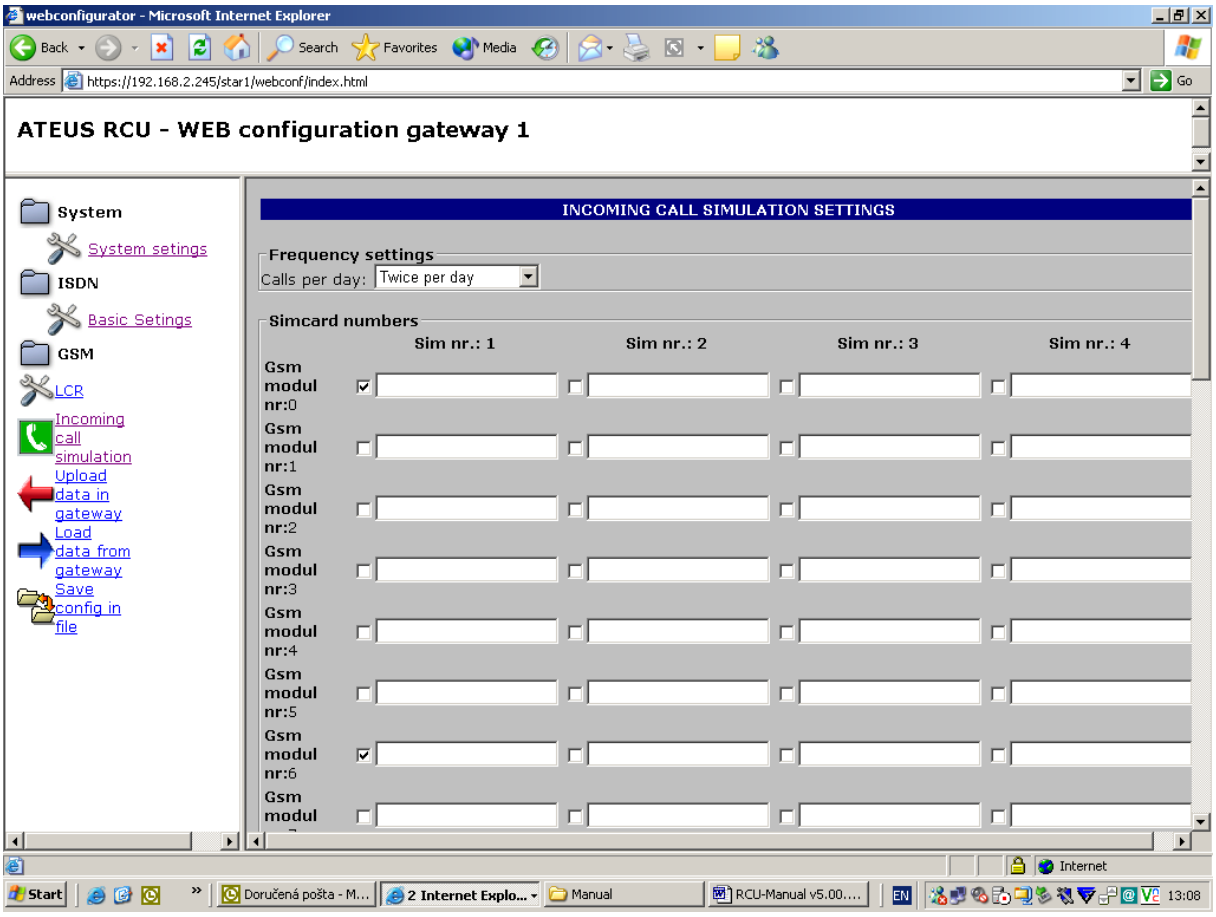

Fig.14: Incomming Call Simulation (ICS)

5.2 SNMP Management

Users operating a network management system either locally or by outsourcing can readily incorporate the RCU in to their network management software (HP OpenView, Tivoli, Netcool … etc) and enjoy the convenient services of the SNMP protocol.

5.2.1 SNMP Queries

The PRI GSM gateway MIB has to be properly installed in the Network Management Node (NMN). This installation is beyond the scope of this manual (help can be sought from the 2N technical support stuff). When all is installed, SNMP queries can be send from the NMN to the RCU on all the SNMP objects in the PRI GSM gateway MIB. Different gateways are represented by their SNMP IP addresses (Eth0, Eth0:1, …, Eth0:n).

5.2.2 SNMP Traps

Immediately after configuration, the RCU begins to send event driven alarms to announce changes in the different statuses of the PRI GSM gateway. Each trap is again identified by the

source address, which corresponds to the SNMP IP address of the respective PRI GSM gateway (Fig.15)

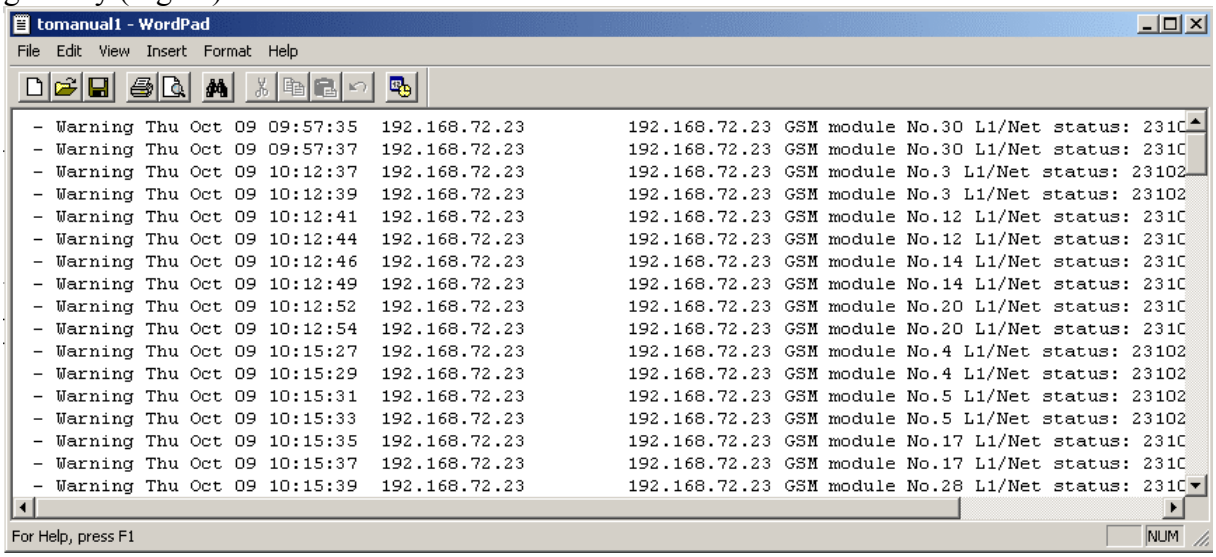

Fig.15: RCU alarms (traps)

5.3 Accounting

Besides PRI GSM gateway management, the RCU collects different accounting information. This information can be thereafter retrieved at the discretion of the user in two ways. The first method employs the web interface as has already been mentioned in section 5.1.3. In the second method, we use a Secure Shell (SSH) client to download the accounting data directly from the RCU. All accounting information for individual PRI GSM gateways is stored in the **/var/log** directory (Fig. 16). If you, for example, wish to retrieve accounting information on gateway 0, please connect to the RCU by SSH and move to */var/log/stargate0*. This directory contains specific accounting information for gateway 0. Billing information (CDR) is stored in files of the form *b-yyyy-mm-dd.log*. An example is *b-2003-09-18.log* i.e. the CDR for 18th of September 2003.The other useful information is found in the trace files. They too have a similar format *t-yyyy.mm.dd.log*. You will find a lot of other information useful for troubleshooting when something goes wrong. These include logs and error messages.

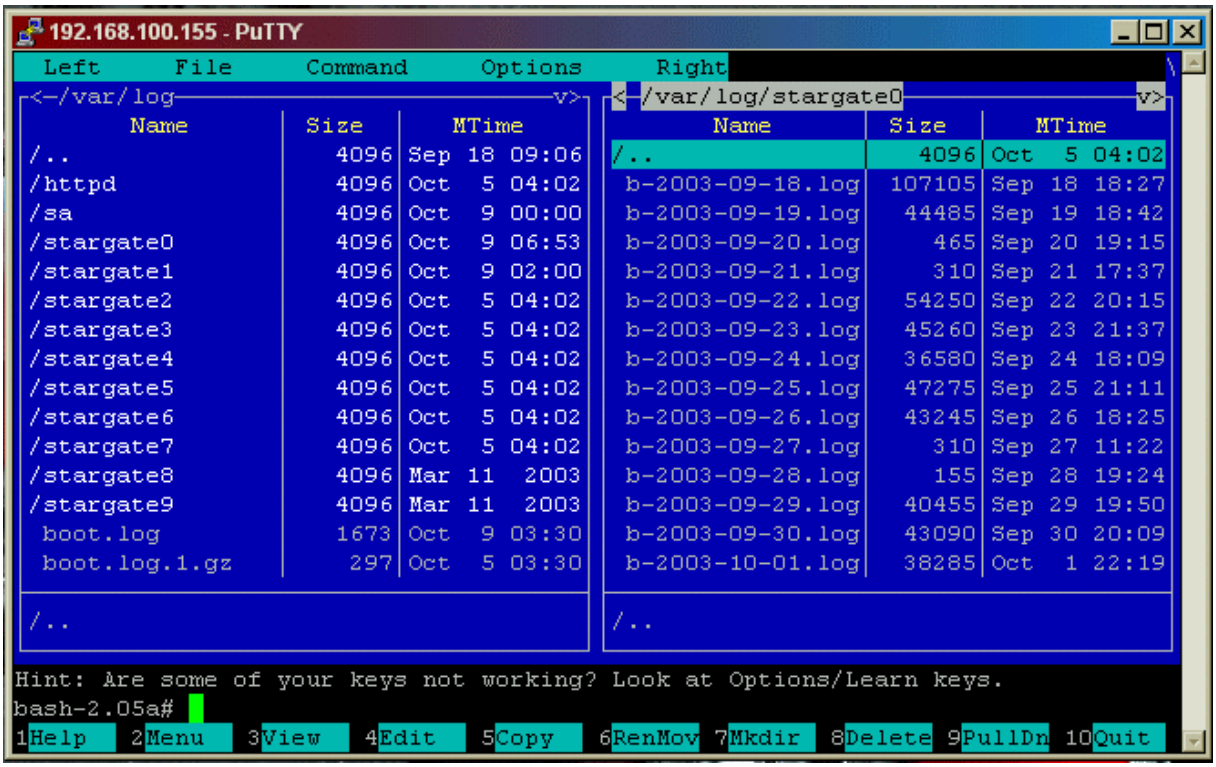

Fig.16: RCU accounting data.

6 Troubleshooting

Installing and configuring a system so as to satisfy the expected functionality is only the part of the show. The real challenge is in keeping the system working. The RCU is no exception in this regard, what is worse, there does not exist a question-answer cook book for solving all the possible combinations of error states that may befall the RCU. A lot depends on the ability of the system administrator to troubleshoot and closely follow all leads towards the resolution of the problem. The following sections elaborate on the tools that can be used in troubleshooting the RCU.

6.1 Stargate Service

The *stargate service* is a set of scripts that control the overall functionality of the RCU system. These scripts include:

Script	Function
sgethsvr	Communicates with the gateways by TELNET (Needs Ethernet connectivity)
sgagent	Responsible for the automatic download of statuses and CDRs
sgtrace	Responsible for the automatic download of traces.
sglcr	Takes care of external routing
snmpd	Communicates with the management station by the SNMP protocol

Just like any other Linux script in **/etc/rc.d/init.d/,** the stargate service has the following parameters.

- *Status* – whether the gateway scripts are running or stopped
- *Start* – start the gateway scripts
- *Stop* – stop the gateway scripts
- *Restart* – First stops the gateway scripts and then starts them. Please restart the gateway scripts every time you change the RCU configuration.

Method1:

bash-2.05a#
bash-2.05a# service stargate {status | start | stop | restart }

Method2:

bash-2.05a#
bash-2.05a# /etc/rc.d/init.d/stargate {status | start | stop | restart }

When the RCU is not working properly, use the stargate service status to check whether all the expected services are running. Do stargate service restart every time you change the RCU configuration.

6.2 Gateway configuration (sgconf)

This script displays the configured Gateways and their corresponding IP addresses.

bash-2.05a#
bash-2.05a# sgconf

The output of this command can be used against the pre-installation IP map to check whether the gateway ordering and configuration are in agreement.

6.3 Checking the Databases

6.3.1 Gateway Databases

The RCU has a total of 21 databases:

- Databases stargate0–9 store status information from gateways 0-9.
- Databases conf0–9 store web configuration data of gateways 0-9.
- Routing Database - a database of prefixes for external routing

6.3.2 Gateway Terminal (sgterm)

The sgterm script is used to send AT commands to the individual gateways from the RCU. A user sitting in the office can connect to the RCU by SSH and use the sgterm to send AT commands to any PRI GSM gateway connected to the RCU. Sgterm takes the gateway number (database number) as the first parameter and an AT command as the second one. For instance, to send an AT command to get the processor serial number of the first unit (stargate0) you would use the following command:

bash-2.05a#
bash-2.05a# sgterm 0 “ati4“
This sends the AT command “ati4” to Stargate0.

If an AT command contains the character “**!**”, please place a “\” before “**!**”.

bash-2.05a#
bash-2.05a# sgterm 0 at\!q
This command sends the AT command “at!q“ to the Stargate0.

The Gateway terminal can be used to troubleshoot the databases, i.e., to test whether the databases are updating properly.

6.3.3 Accessing table main

Table below shows the structure of table “main“ in databases stargate0-9 and the corresponding AT commands that can be used to crosscheck values of the table fields. This table contains the basic configuration and status information from the corresponding gateway.

Id	Description	sgterm 0-9	Meaning
0	Gateway’s CPU serial number	ATI4	
1	Bootware and Firmware versions	ATI3	
2	Stargate IP address	AT&V, S70	
3	Gateway IP netmask	AT&V, S71	
4	Mode of routing	AT&V, S90	0 = cyclic

	outgoing calls (ISDN to GSM)		1 = Locked 2 =According to credit
5	Saving call data CDRs	AT&V, S91	0 = no calls 1 = successful outgoing 2 = successful incoming 3 = successful incoming + outgoing 4 = not used 5 = all outgoing 6 = all incoming 7 = all incoming + outgoing
6	Number of GSM boards in the Gateway		
7	Time and date	AT&V, S99	
8	PIN	AT&V, S98	
9	CPU type	ATI4	
10	CPU utilization	AT! P	
11	Serial port status		
12	Ethernet port status		
13	Trace mode	AT&V, S92	0-32, 1 = layers 3&4, 9 = layers 2,3&4 …
14	Type of AUX board	AT&SAX	
15	Status of AUX board	AT&SAX	
16	Status of AUX layer 3	AT&SAX	
17	Type of PRI board	AT&SPR	
18	Status of PRI board	AT&SPR	
19	PRI1 - Mode of PRI interface	AT&VI	TE/S = TE, Slave TE/M = TE, Master NT/S = NT, Slave NT/M = NT, Master QSIG/M = QSIG, Master QSIG/S = QSIG, Slave
20	PRI1 - TEI Number	AT&VI, I01	
21	Not used		
22	PRI1 - ISDN layer1	AT&SPR	Stargate or Bluestar user manual
23	PRI1 - ISDN layer2	AT&SPR	
24	PRI1 - ISDN layer3	AT&SPR	
25	PRI1 - Number of current calls	AT&XC, AT&XP, AT&XG	
26	PRI1 - Max. Number of simultaneous calls		
27	PRI1 - reject causes	AT&VI, I05	
28	PRI2 - Mode of PRI interface	AT&VI	TE/S = TE, Slave TE/M = TE, Master NT/S = NT, Slave

			NT/M = NT, Master QSIG/M = QSIG, Master QSIG/S = QSIG, Slave
29	PRI2 - TEI Number	AT&VI, I01	
30	Not used		
31	PRI2 - ISDN layer1	AT&SPR	Stargate or Bluestar user manual
32	PRI2 - ISDN layer2	AT&SPR	
33	PRI2 - ISDN layer3	AT&SPR	
34	PRI2 - Number of current calls	AT&XC, AT&XP, AT&XG	
35	PRI2 - Max. Number of simultaneous calls		
36	PRI2 - reject causes	AT&VI, I05	

To retrieve the contents of main for a particular Gateway, you should.

- Connect to database – **psql** db-name (db-name can be one of stargate0-9)
- Display the contents of table "main" ordered by "id" – **select * from main order by id;**

Further useful commands are:

- Exit database - **\q**
- List all the databases in the system - **\l**
- List all the tables in the database - **\d**
- Help! - **\help**
- Export database "db-name" to a file "f-name" – **pg_dump db-name > f-name**

To troubleshoot the databases, retrieve the contents of the databases and check them against the output of AT commands using the sgterm as in the table above.

6.4 Stargate (Bluestar) Program using RCU as a tunnel

RCU also provides a possibility to safely connect directly to each PRI GSM Gateway using Stargate/Bluestar program. It could be done using application (tool) *putty.exe,* included in Your User's Guide CD, or downladable for free from Internet. What should be done to make this work?

Step 1: In the putty Session window (Fig. 17), set host name (IP address) and port 22 (SSH)

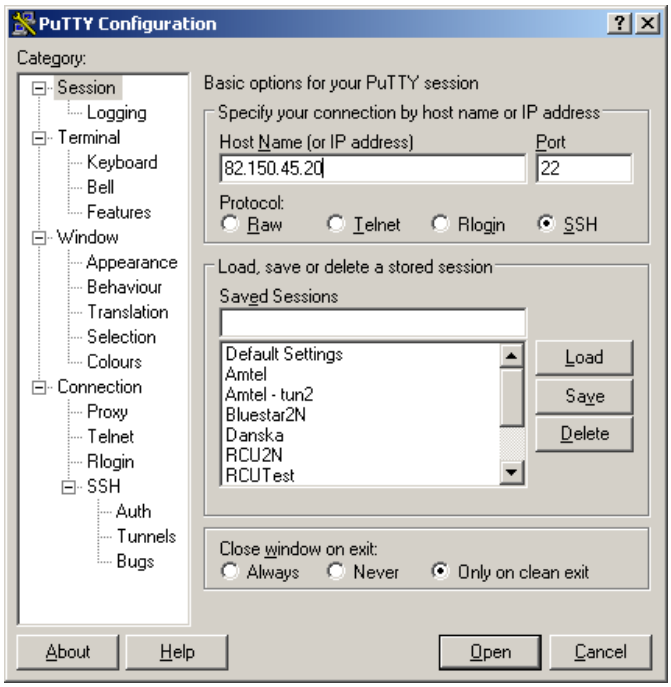

Fig. 17: Setting IP address and port

Step 2: In the putty menu choose Connection – SSH – Tunnels (Fig. 18). Configure forwarding of a local TCP port (it could be 23 or different) to port 23 (Telnet) of the related PRI GSM gateway. Here you must fill the private IP address of the related PRI GSM gateway.

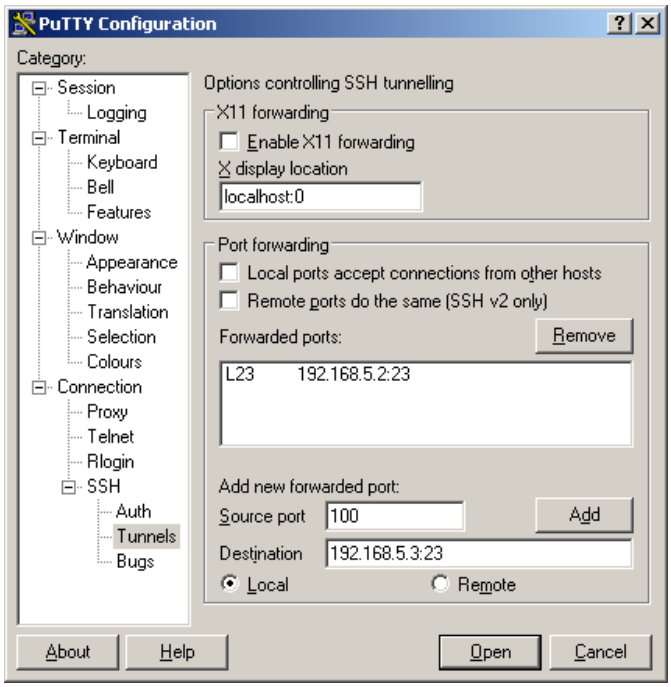

Fig. 18: Configuring a tunnel

Step 3: Save this session under some name.

Step 4: Open this session and log to the RCU

Step 5: In the Stargate/Bluestar program, in the list of gateways, add a gateway with IP address 127.0.0.1 and the same port configured as a local port in putty.

Step 6: Connect to the new added gateway

If You forward more ports in *putty*, You can connect to a few gateways at the same time using separate Stargate/Bluestar Progam sessions!

This way You can use all Stargate/Bluestar Program functions as connected to gateway directly by Telnet.

6.5 Tracing of the traffic on gateways

The gateway traffic tracing is very usefull feature that make troubleshooting much easier and efficient, then it should be without it. The trace is logged in daily made files, that provides solving problems reported on the specified date easy to locate.

If you want to stop all-time tracing on certain gateway, just disable it creating an empty file:

touch /var/run/stargate/disable_trace_n

where *n* is the gateway order number {0,1,2…,7}.

To enable it, just delete the file:

rm /var/run/stargate/disable_trace_n

Tracing is enabled by default.

7 FAQ

Q1: All connected gateways do not communicate with the RCU
A1: 1-check IP connectivity (ping)
2-make sure that service stargate scripts are running
3-use sgconf to confirm the right configuration and gateway ordering

Q2: There is IP connectivity but cannot login to the webview
A2: Re-run "webpass" and remember your username and password

Q3: There is IP connectivity but the webview displays "STARGATE NOT CONNECTED"
A1: 1-check 2&3 in Q1
2-check that the serial number of your gateway CPU is the same as the one at the backside of your RCU CD

Q4: IP connectivity works, but the web view displays "STARGATE NOT CONNECTED" and the log file contains "Call service"
A4: Check which CPU number (STARGATE or BLUESTAR) is connected to which database and compare it with information received on acompaning letter received with Your RCU:

Database Number	CPU Serial Number	Key Code 1	Key Code 2	Key Code3
0	<CPU from gateway 0>	…		
1	<CPU from gateway 1>	…		

Q5: How to disable/enable tracing of the traffic on the gateway?
A5:

1. Disable – Create an empty file:

touch /var/run/stargate/disable_trace_*n*

where is *n* – gateway order number {0,1,2…,7}

2. Enable – Delete the file:

rm /var/run/stargate/disable_trace_*n*

Appendix 1: The Trap Table

Base OID:						
1.3.6.1.4.1.6530.0						
Trap ID	Source MIB Object	Event	Form	The Event Log Message in HP OpenView NNM definition	Severity	Related trap
501	sgCPUBoard.sgcpuStatus.sgcpuSerialPort	a value change to NOK	No response from serial port	No response from serial port	Critical	502
502	sgCPUBoard.sgcpuStatus.sgcpuSerialPort	a value change to OK	Serial communication restored	Serial communication restored	Major	501
503	sgCPUBoard.sgcpuStatus.sgcpuCPUUtilization	a value increased to > 80	CPU Utilization : <Source MIB Object Value>	CPU Utilization : $1	Major	504
504	sgCPUBoard.sgcpuStatus.sgcpuCPUUtilization	a value decreased to < 60	CPU Utilization : <Source MIB Object Value>	CPU Utilization : $1	Warning	503
511	sgAUXBoard.sgauxType	a value change to NONE	AUX board missing	AUX board missing	Major	512
512	sgAUXBoard.sgauxType	a value change to <>NONE	AUX board inserted	AUX board inserted	Warning	511
513	sgAUXBoard.sgauxGeneralStatus	a value change to <>OK	AUX board status: <Source MIB Object Value>	AUX board status: $1	Major	514
514	sgAUXBoard.sgauxGeneralStatus	a value change to OK	AUX board status: OK	AUX board status: OK	Warning	513
521	sgPRIBoard.sgpriType	a value change to NONE	PRI board missing	PRI board missing	Critical	522
522	sgPRIBoard.sgpriType	a value change to <>NONE	PRI board inserted	PRI board inserted	Major	521
523	sgPRIBoard.sgpriGeneralStatus	a value change to <>OK	PRI board status: <Source MIB Object Value>	PRI board status: $1	Major	524
524	sgPRIBoard.sgpriGeneralStatus	a value change to OK	PRI board status: OK	PRI board status: OK	Warning	523
525	sgPRIBoard.sgPRI1Status.sgpri1Layer1/net or sgPRIBoard.sgPRI2Status.sgpri2Layer1/net	a value change to <>ACTIVE	PRI <port number> link unplugged	PRI - $1 link unplugged	Critical	526
526	sgPRIBoard.sgPRI1Status.sgpri1Layer1/net or sgPRIBoard.sgPRI2Status.sgpri2Layer1/net	a value change to ACTIVE	PRI <port number> link plugged in	PRI - $1 link plugged in	Major	525
527	sgPRIBoard.sgPRI1Status.sgpri1Layer2 or sgPRIBoard.sgPRI2Status.sgpri2Layer2	a value change to <>OKEST	PRI <port number> Multiple frame Not Established	PRI - $1 Multiple frame Not Established	Minor	528
528	sgPRIBoard.sgPRI1Status.sgpri1Layer2 or sgPRIBoard.sgPRI2Status.sgpri2Layer	a value change to OKEST	PRI <port number> Multiple frame Established	PRI - $1 Multiple frame Established	Warning	527

529	sgPRIBoard.sgPRI1Status.sgpri1BusyBChanCurrent or sgPRIBoard.sgPRI2Status.sgpri2BusyBChanCurrent	a value increased over <high_up limit> value defined in sgsetup session	PRI <port number> Number of busy B channels increased to <Source MIB Object Value>	PRI - $1 Number of busy B channels increased to $2	Warning	530
530	sgPRIBoard.sgPRI1Status.sgpri1BusyBChanCurrent or sgPRIBoard.sgPRI2Status.sgpri2BusyBChanCurrent	a value decreased under <high_down limit> value defined in sgsetup session	PRI <port number> Number of busy B channels decreased to <Source MIB Object Value>	PRI - $1 Number of busy B channels decreased to $2	Warning	529
531	sgPRIBoard.sgPRI1Status.sgpri1BusyBChanCurrent or sgPRIBoard.sgPRI2Status.sgpri2BusyBChanCurrent	a value decreased under <low_down limit> value defined in sgsetup session	PRI <port number> Number of busy B channels decreased to <Source MIB Object Value>	PRI - $1 Number of busy B channels decreased to $2	Minor	532
532	sgPRIBoard.sgPRI1Status.sgpri1BusyBChanCurrent or sgPRIBoard.sgPRI2Status.sgpri2BusyBChanCurrent	a value increased over <low_up limit> value defined in sgsetup session	PRI <port number> Number of busy B channels increased to <Source MIB Object Value>	PRI - $1 Number of busy B channels increased to $2	Warning	531
541	sgGSMBoardTab.sgGSMBoardEntry.sgbType	a value change to NONE	GSM board in slot <SlotNumber> missing	GSM board in slot $1 missing	Major	542
542	sgGSMBoardTab.sgGSMBoardEntry.sgbType	a value change to <>NONE	GSM board in slot <SlotNumber> inserted	GSM board in slot $1 inserted	Warning	541
543	sgGSMBoardTab.sgGSMBoardEntry.sgbGeneralStatus	a value change to <>OK	GSM board in slot <SlotNumber> status: <Source MIB Object>	GSM board in slot $1 status: $2	Major	544
544	sgGSMBoardTab.sgGSMBoardEntry.sgbGeneralStatus	a value change to OK	GSM board in slot <SlotNumber> status: OK	GSM board in slot $1 status: OK	Warning	543
551	sgGSMModuleTab.sgGSMModuleEntry..sgmSignalLevel	a value change to < -100	GSM module <ModuleNumber> status: Low signall	GSM module $1 status: Low signall	Warning	552
552	sgGSMModuleTab.sgGSMModuleEntry.sgmSignalLevel	a value change to > - 95	GSM module <ModuleNumber> status: Signall OK	GSM module $1 status: Signall OK	Warning	551
553	sgGSMModuleTab.sgGSMModuleEntry.sgmLayer1/net	any value change	GSM module <ModuleNumber> Layer1/net status: <Source MIB Object Value>	GSM module $1 Layer1/net status: $2	Warning	553
554	SgGSMModuleTab.sgGSMModuleEntry.sgmLayer2	any change between irregular states or between irregular and regular state	GSM module <ModuleNumber> Layer2 status: <Source MIB Object Value>	GSM module $1 Layer2 status: $2	Warning	554
555	SgGSMModuleTab.sgGSMModuleEntry.sgmSIMxASR (According to ASR definition chosen insgsetup)	a value decreased under <Low ASR> value defined in sgsetup session>	GSM Module <Module Number>: Call success rate LOW: <Source MIB Object Value>	GSM module $1 : Low ASR: $2	Major	556

556	SgGSMModuleTab.sgGSMModuleEntry.sgmSIMxASR (According to ASR definition chosen in sgsetup)	a value increased over <Good ASR> value defined in sgsetup session>	GSM Module <Module Number : Call success rate OK: <Source MIB Object Value>	GSM module $1: ASR OK: $2	Warning	555